DIOPHANTINE DEFINABILITY AND DECIDABILITY IN THE EXTENSIONS OF DEGREE 2 OF TOTALLY REAL FIELDS

ALEXANDRA SHLAPENTOKH

Abstract. We investigate Diophantine definability and decidability over some subrings of algebraic numbers contained in quadratic extensions of totally real algebraic extensions of $\mathbb{Q}$. Among other results we prove the following. The big subring definability and undecidability results previously shown by the author to hold over totally complex extensions of degree 2 of totally real number fields, are shown to hold for *all* extensions of degree 2 of totally real number fields. The definability and undecidability results for integral closures of "small" and "big" subrings of number fields in the infinite algebraic extensions of $\mathbb{Q}$, previously shown by the author to hold for totally real fields, are extended to a large class of extensions of degree 2 of totally real fields. This class includes infinite cyclotomics and abelian extensions with finitely many ramified rational primes.

1. Introduction

The interest in the questions of existential definability and decidability over rings goes back to a question that was posed by Hilbert: given an arbitrary polynomial equation in several variables over $\mathbb{Z}$, is there a uniform algorithm to determine whether such an equation has solutions in $\mathbb{Z}$? This question, otherwise known as Hilbert's Tenth Problem, has been answered negatively in the work of M. Davis, H. Putnam, J. Robinson and Yu. Matiyasevich. (See [4] and [5].) Since the time when this result was obtained, similar questions have been raised for other fields and rings. In other words, let R be a recursive ring. Then, given an arbitrary polynomial equation in several variables over R, is there a uniform algorithm to determine whether such an equation has solutions in R? One way to resolve the question of Diophantine decidability negatively over a ring of characteristic 0 is to construct a Diophantine definition of $\mathbb{Z}$ over such a ring. This notion is defined below.

Definition 1.1. Let R be a ring and let $A \subset R$. Then we say that A has a Diophantine definition over R if there exists a polynomial $f(t, x_1, \ldots, x_n) \in R[t, x_1, \ldots, x_n]$ such that for any $t \in R$,

$$\exists x_1, \ldots, x_n \in R, f(t, x_1, ..., x_n) = 0 \Longleftrightarrow t \in A.$$

If the quotient field of R is not algebraically closed, we can allow a Diophantine definition to consist of several polynomials without changing the nature of the relation. (See [5] for more details.)

The usefulness of Diophantine definitions stems from the following easy lemma.

Lemma 1.2. *Let $R_1 \subset R_2$ be two recursive rings such that the quotient field of R_2 is not algebraically closed. Assume that Hilbert's Tenth Problem (abbreviated as "HTP" in the future) is undecidable over R_1, and R_1 has a Diophantine definition over R_2. Then HTP is undecidable over R_2.*

Using norm equations, Diophantine definitions have been obtained for $\mathbb{Z}$ over the rings of algebraic integers of some number fields. Jan Denef constructed a Diophantine definition of $\mathbb{Z}$ for the finite degree totally real extensions of $\mathbb{Q}$. Jan Denef and Leonard Lipshitz extended Denef's results to all the extensions of degree 2 of the finite degree totally real fields. Thanases Pheidas and the author of this paper have independently constructed Diophantine definitions of $\mathbb{Z}$ for number fields with exactly one pair of non-real conjugate embeddings. Finally Harold N. Shapiro and the author of this paper showed that the subfields of

Date: June 02, 2006.

2000 *Mathematics Subject Classification.* Primary 11U05; Secondary 03D35.

Key words and phrases. Hilbert's Tenth Problem, norm equations, Diophantine definitions.

The research for this paper has been partially supported by NSF grant DMS-0354907 and ECU Faculty Senate Summer 2005 Research Grant.

all the fields mentioned above "inherited" the Diophantine definitions of $\mathbb{Z}$. (These subfields include all the abelian extensions.) The proofs of the results listed above can be found in [6], [8], [7], [14], [20], and [22]. The author also showed that the totally real fields which are non-trivial extensions of $\mathbb{Q}$, and the totally complex extensions of degree 2 of the totally real fields contain "big" rings, i.e. rings consisting of algebraic numbers with infinitely many primes allowed in the denominators of divisors, where $\mathbb{Z}$ is definable and Hilbert's Tenth Problem has no solution. The details of these results can be found in [25], [23] and [28]. Subsequently these results were extended by the author to the integral closures of some rings of $\mathscr{S}$-integers where $\mathscr{S}$ is finite (in the future referred to as "small" rings) and to the integral closures of some "big" rings in a class of infinite totally real extensions of $\mathbb{Q}$ (see [24] and [30].)

The investigation of "big" rings was prompted by difficulties of resolving the status of Hilbert's Tenth Problem over $\mathbb{Q}$. These difficulties, in part, gave rise to a series of conjectures by Barry Mazur which can be found in [10], [11], [12], and [13]. The strongest of the conjectures in [10] was refuted in [1], but the status of the other conjectures as well as the Diophantine status of $\mathbb{Q}$ and other number fields is still unknown. Among other things, Mazur's conjectures implied that infinite discrete (in Archimedean or $\mathfrak{p}$-adic topology) sets are not existentially definable over $\mathbb{Q}$ (or other number fields) and thus $\mathbb{Z}$ is not Diophantine over $\mathbb{Q}$. Cornelissen and Zahidi showed that one of the conjectures also implied that another possible method of proof of Diophantine undecidability of $\mathbb{Q}$ was not viable, i.e. they showed that one of Mazur's conjectures implied that there was no Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$. (See [3] for more information on this result.)

In arguably the most important development in the subject since the solution of the original problem, Poonen showed that there exist "really big" recursive subrings of $\mathbb{Q}$ (that is recursive subrings with the natural density of primes allowed in the denominators equal to 1), where one could construct an infinite, existentially definable over the ring discrete in archimedean topology set, which is also a Diophantine model of $\mathbb{Z}$. Thus, Poonen showed that a ring version of a Mazur's conjecture failed for this ring and Hilbert's Tenth Problem was undecidable over the ring. (See [17] for more details.) In a paper joint with the author (see [18]), this result was lifted to any number field which has a rank one elliptic curve. Poonen and the author also showed in [18] that some "really big" subrings of number fields with a rank one elliptic curve ($\mathbb{Q}$ being one of these fields) had Diophantine sets which were simultaneously discrete in the usual archimedean and every non-archimedean topology of the field. Additionally, the paper contained examples of "big" rings with $\mathfrak{p}$-adically discrete Diophantine sets contained in totally real number fields and their totally complex extensions of degree 2.

Elliptic curves have also been used to show undecidability of rings of algebraic integers. The first use of elliptic curves for this purpose is due to Denef who proved the following proposition in [8].

Theorem 1.3. *Let K_∞ be a totally real algebraic possibly infinite extension of $\mathbb{Q}$. If there exists an elliptic curve $\mathscr{E}$ over $\mathbb{Q}$ such that $[\mathscr{E}(K) : \mathscr{E}(\mathbb{Q})] < \infty$, then $\mathbb{Z}$ has a Diophantine definition over the rings of algebraic integers of K.*

Extending ideas of Denef, Bjorn Poonen has shown the following in [16].

Theorem 1.4. *Let M/K be a number field extension with an elliptic curve $\mathscr{E}$ defined over K, of rank one over K, such that the rank of $\mathscr{E}$ over M is also one. Then O_K (the ring of integers of K) is Diophantine over O_M.*

In a recent paper (see [2]), Cornelissen, Pheidas and Zahidi weakened somewhat assumptions of Poonen's theorem. Instead of requiring a rank 1 curve retaining its rank in the extension, they require existence of a rank 1 elliptic curve over the bigger field and an abelian variety over the smaller field retaining its rank in the extension. Further, Poonen and the author have independently shown that the conditions of Theorem 1.4 can be weakened to remove the assumption that rank is one and require only that the rank in the extension is the same (see [21] and [15]). In [21], the author also showed that the elliptic curve technique extends to "big rings".

In this paper, using norm equations, we extend the "big" ring results to *all* extensions of degree two of totally real number fields and some totally real infinite extensions of $\mathbb{Q}$. In the case of infinite extensions, we will all also obtain new results for rings of $\mathscr{S}$-integers but not for rings of integers. (Corresponding results

for rings of integers can be obtained via elliptic curve methods as in [21]. We intend to do this in the future.) En route to the results above we obtain improvements relative to [30] for the results concerning "big" and "small" rings of some totally real infinite extensions of $\mathbb{Q}$, as well as results on integrality at finitely many "primes" in infinite extensions. The main theorems of the paper are stated below.

Theorem. Let G be an extension of degree 2 of a totally real number field. Then for any $\varepsilon > 0$ there exists a set $\mathscr{V}_G$ of primes of G whose natural density is bigger than $1 - 1/[G : \mathbb{Q}] - \varepsilon$ and such that $\mathbb{Z}$ has a Diophantine definition over $O_{G,\mathscr{V}_G}$.

Theorem. Let A_∞ be an abelian (possibly infinite) extension of $\mathbb{Q}$ with finitely many ramified primes. Then the following statements are true.

- If the ramification degree of 2 is finite, then for any number field $A \subset A_\infty$ there exists an infinite set of A-primes $\mathscr{W}_A$ such that $\mathbb{Z}$ is existentially definable in the integral closure of $O_{A,\mathscr{W}_A}$ of A_∞.
- For any number field $A \subset A_\infty$ and any finite non-empty set $\mathscr{S}_A$ of its primes, we have that $\mathbb{Z}$ is existentially definable in the integral closure of $O_{A,\mathscr{S}_A}$ in A_∞.

Theorem. Let q be a rational prime. Let L be an algebraic, possibly infinite extension of $\mathbb{Q}$. Let $\mathfrak{P}_L$ be a prime of L (a prime ideal of O_L – the ring of algebraic integers of L) such that it is relatively prime to q (meaning the ideal does not contain q), the residue field of $\mathfrak{P}_L$ has an extension of degree q, and for any number field $M \subset L$, it is the case that any M-prime $\mathfrak{p}_M$ lying below $\mathfrak{P}_L$ is unramified over $\mathbb{Q}$. Then for any number field $M \subset L$, there exists a subset $\mathscr{X}$ of L satisfying the following conditions:

- If $x \in \mathscr{X}$, then x is integral with respect to $\mathfrak{p}_M$, an M-prime below $\mathfrak{P}_L$.
- If $x \in M$ and x is integral at $\mathfrak{p}_M$, then $x \in \mathscr{X}$.
- $\mathscr{X}$ is Diophantine over L.

2. **Preliminary Results.**

In this section we state some definitions and a few well-known technical propositions which will be used in the proofs. We start with a definition of "big" rings and integrality at finitely many primes in a number field.

Definition 2.1. Let K be a number field. Let $\mathscr{W}_K$ be a set of its non-archimedean primes. Then define

$$O_{K,\mathscr{W}_K} = \{x \in K : \mathrm{ord}_{\mathfrak{p}} x \geq 0, \forall \mathfrak{p} \notin \mathscr{W}_K\}.$$

If $\mathscr{W}_K$ is empty the ring $O_{K,\mathscr{W}_K} = O_K$ is the ring of integers of K. If $\mathscr{W}_K$ is finite, then the ring $O_{K,\mathscr{W}_K}$ is called the ring of $\mathscr{W}_K$-integers or a "small" ring. If $\mathscr{W}_K$ is infinite, we will call the ring $O_{K,\mathscr{W}_K}$ a "big" ring.

Proposition 2.2. *Let K be a number field. Let $\mathscr{W}_K$ be any set of primes of K. Let $\mathscr{S}_K \subseteq \mathscr{W}_K$ be a finite set. Let $\mathscr{V}_K = \mathscr{W}_K \setminus \mathscr{S}_K$. Then $O_{K,\mathscr{V}_K}$ has a Diophantine definition over $O_{K,\mathscr{W}_K}$. (See, for example,* [23]*.)*

Next we state another technical proposition which is also quite important for the proofs in this paper.

Proposition 2.3. *Let K be a number field. Let $\mathscr{W}_K$ be any set of primes of K. Then the set of non-zero elements of $O_{K,\mathscr{W}_K}$ has a Diophantine definition over $O_{K,\mathscr{W}_K}$. Further, let K_∞ be an algebraic extension of K and let $O_{K_\infty,\mathscr{W}_{K_\infty}}$ be the integral closure of $O_{K,\mathscr{W}_K}$ in K_∞. Then the set of non-zero elements of $O_{K_\infty,\mathscr{W}_{K_\infty}}$ has a Diophantine definition over $O_{K_\infty,\mathscr{W}_{K_\infty}}$ (See, for example,* [23] *and* [30]*.)*

We will also need the following easy proposition:

Proposition 2.4. *Let F be an algebraic extension of $\mathbb{Q}$. Let O_F be the ring of integers of F. Then the following set of pairs of elements of O_F is Diophantine over O_F: $\{(a, b) \in (O_F)^2 : (a, b) = 1\}$.*

Proof. It is enough to note that $(a, b) = 1 \Leftrightarrow (\exists A, B \in O_F)(Aa + Bb) = 1$. □

The following proposition will allow us to set up bounds for real valuations.

Proposition 2.5. *Let F be an algebraic extension of $\mathbb{Q}$. Let $P = \{x \in F |$ For all embeddings $\sigma : F \longrightarrow \mathbb{R}, \sigma(x) \geq 0\}$. Then P is Diophantine over F. (See [8], Lemma 10.)*

The next proposition deals with rewriting equations using variables from finite degree subfields.

Proposition 2.6. *Let F_2/F_1 be a finite field extension. Let $R_1 \subseteq F_1$ be a ring whose fraction field is F_1 and let R_2 be the integral closure of R_1 in F_2. Assume further that the set of non-zero elements is Diophantine over R_1. Let*

$$P(X_1, \ldots, X_n, z_1, \ldots, z_m) = 0 \tag{2.1}$$

be an equation with coefficients in F_2. Then for some positive integers l and r, there exists a system of equations

$$\{Q_i(t_1, \ldots, t_r, z_1, \ldots, z_m) = 0, i = 1, \ldots, l\} \tag{2.2}$$

over R_1 such that (2.2) has solutions $t_1, \ldots, t_r, z_1, \ldots, z_m \in R_1$ if and only if (2.1) has solutions $X_1, \ldots, X_n$ in R_2, $z_1, \ldots, z_m \in R_1$.

Proof. The rewriting proceeds in several steps. First of all let $\{\omega_1, \ldots, \omega_k\}$ be a basis of F_2 over F_1. Let

$$P(X_1, \ldots, X_n, z_1, \ldots, z_m) = \sum_{i_1, \ldots, i_n, e_1, \ldots, e_m} A_{i_1, \ldots, i_n, e_1, \ldots, e_m} X_1^{i_1} \ldots X_n^{i_n} z_1^{e_1} \ldots z_m^{e_m} = 0. \tag{2.3}$$

Next note that $A_{i_1, \ldots, i_n} = \sum_{j=1}^{k} b_{i_1, \ldots, i_n, e_1, \ldots, e_m, j} \omega_j$, where $b_{i_1, \ldots, i_n, j} \in F_1$. Now we replace (2.3) by

$$\sum_{i_1 \ldots i_n, e_1 \ldots e_m} \left(\sum_{j=1}^{k} b_{i_1, \ldots, i_n, e_1, \ldots, e_m, j} \omega_j \right) \left(\sum_{j=1}^{k} x_{1,j} \omega_j \right)^{i_1} \ldots \left(\sum_{j=1}^{k} x_{n,j} \omega_j \right)^{i_n} z_1^{e_1} \ldots z_m^{e_m} = 0. \tag{2.4}$$

The next step is to make sure that for each i we have that $\sum_{j=1}^{k} x_{i,j} \omega_j$ is in the integral closure of R_1 and all the variables range over R_1. To reach the latter goal we will replace each $x_{i,j}$ by a ratio $u_{i,j}/v_{i,j}$ where $u_{i,j}, v_{i,j}$ will range over R_1. To insure that $\sum_{j=1}^{k} (u_{i,j}/v_{i,j}) \omega_j$ is in R_2, the integral closure of R_1 in F_2, we add an equation requiring that the all the symmetric functions of the conjugates of the sum over F_1 are in R_1 or alternatively that the coefficients of the characteristic polynomial are all in R_1. We also add equations stating that $v_{i,j} \neq 0$ as elements of R_1.

The third step is multiply all the factors out treating $z_j, u_{i,j}/v_{i,j}$'s as elements of F_1 and to replace products of the elements of the basis by their linear combinations over F_1. This operation will produce a linear combination of ω's with coefficients which are polynomials in $u_{i,j}/v_{i,j}$. The last step is then to multiply by appropriate powers of $v_{i,j}$'s and denominators of $b_{i_1, \ldots, i_n, e_1, \ldots, e_m, j}$ with respect to R_1 to clear all the denominators. □

Now we state a slightly different version of the rewriting proposition whose proof is completely analogous to the proof above.

Proposition 2.7. *Let F_2/F_1 be a finite field extension. Let $R_1 \subseteq F_1$ be a ring whose fraction field is F_1 and let $R_2 = R_1[\nu]$, where ν generates F_2 over F_1 and ν is integral over R_1. Let*

$$P(X_1, \ldots, X_n, z_1, \ldots, z_m) = 0 \tag{2.5}$$

be an equation with coefficients in F_2. Then for some positive integers l and r, there exists a system of equations

$$\{Q_i(t_1, \ldots, t_r, z_1, \ldots, z_m) = 0, i = 1, \ldots, l\} \tag{2.6}$$

over R_1 such that (2.2) has solutions $t_1, \ldots, t_r, z_1, \ldots, z_m \in R_1$ if and only if (2.1) has solutions $X_1, \ldots, X_n$ in R_2, $z_1, \ldots, z_m \in R_1$.

Using similar reasoning, one can also prove the following easy proposition.

Proposition 2.8. *Let $F_1 \subset F_2 \subset F_3$ be a finite extension of number fields. Let $R_1 \subset F_1$ be an integrally closed subring of F_1 such that its fraction field is F_1. Let $\nu_2 \in F_2$ be a generator of F_2 over F_1 such that it is integral over R_1. Similarly, let $\nu_3 \in F_3$ be a generator of F_3 over F_2 such that it is integral over $R_1[\nu_2]$. Let $R_2 = R_1[\nu_2], R_3 = R_1[\nu_2, \nu_3]$. Then for some positive integers l and r there exists a system of polynomial equations*

$$\{Q_i(t_1, \ldots, t_l) = 0, i = 1, \ldots, r\} \tag{2.7}$$

with coefficients in R_1, such that $\mathbf{N}_{F_3/F_2}(\varepsilon) = 1$ has a solution $\varepsilon \in R_3$ if and only if (2.7) has a solution $(t_1, \ldots, t_l) \in R_1^l$.

We finish this section with a notational convention which we will observe throughout the paper.

Notation 2.9. Let $\tilde{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ inside $\mathbb{C}$. All the algebraic extensions of $\mathbb{Q}$ discussed in the paper will be assumed to be subfields of $\tilde{\mathbb{Q}}$. Further, given a finite set of fields $F_1, \ldots, F_k \subset \tilde{\mathbb{Q}}$, we will interpret $F_1 \ldots F_k$ to mean the smallest subfield of $\tilde{\mathbb{Q}}$ containing $F_1, \ldots, F_k$.

3. Integrality at a Prime in Infinite Extensions.

This section contains some technical material necessary for the proofs for the infinite extension cases. However, the result may be of independent interest. More specifically we will discuss existential definability of integrality at finitely many primes in infinite extensions. We will rely heavily on Theorem 2.1 of [27] which is the technical version of the assertion that integrality at finitely many primes is existentially definable over number fields.

Notation and Assumptions 3.1. In this section we will use the following notation and assumptions.

- Let K be a number field.
- Let F be an algebraic (possibly infinite) extension of K.
- Let $q > 2$ be a rational prime number. Let ξ_q be a q-th primitive root of unity.
- Assume $\xi_q \in K$.
- Let $b \in O_K$ and assume that $X^q - b$ is irreducible over F.
- Let $\mathfrak{p}_K$ be a prime of K satisfying the following conditions.
  - $\mathfrak{p}_K$ is not a factor of q.
  - Let $\mathfrak{p}_M$ be any factor of $\mathfrak{p}_K$ in some finite extension M of K such that $M \subset F$. Then $X^q - b$ is irreducible in the residue field of $\mathfrak{p}_M$ and the ramification degree of $\mathfrak{p}_M$ over $\mathfrak{p}_K$ is not divisible by q. We will separate out the case of ramification degree being 1 for all M and all $\mathfrak{p}_M$, and will refer to this case as the "unramified" case. Note also that the irreducibility assumption implies that $\mathrm{ord}_{\mathfrak{p}_M} b = 0$.
- Let $\prod \mathfrak{a}_i^{r_i}$ be the K-divisor of b. For each i, let A_i be the rational prime below $\mathfrak{a}_i$.
- Let $s \geq \max_i\{3qr_i[K : \mathbb{Q}]\}$ be a natural number not divisible by q.
- Let $g \in K$ satisfy the following conditions.
  - $\mathrm{ord}_{\mathfrak{p}_K} g = s \not\cong 0 \mod q$.
  - $g \cong 1 \mod bq^3$.
  - The divisor of g is of the form $\frac{\mathfrak{p}_K^s}{\prod \mathfrak{q}_i^{n_i}}$, where for all i we have that $\mathfrak{q}_i$ is a prime of K such that $\mathfrak{q}_i \neq \mathfrak{p}$ and $n_i \in \mathbb{Z}_{>0}$. (Such a $g \in K$ exists by the Strong Approximation Theorem.)
- Let $r = q^{(3q[K:\mathbb{Q}])}(q^{(q[K:\mathbb{Q}])!} - 1)\left(\prod (A_i^{(q[K:\mathbb{Q}])!} - 1)\right)$
- For $x \in F$, let $h = (q^3 b)^r (g^{-1} x^{r(s+1)} + g^{-q}) + 1$.
- Let $z \in O_K, z \not\cong 0 \mod \mathfrak{p}$.
- Let $\beta(x) \in \tilde{\mathbb{Q}}$ be a root of $T^q - (h^{-1} + z^q)$.
- Let $\beta \in \tilde{\mathbb{Q}}$ be a root of the polynomial $X^q - b$.
- Let $N(a_0, \ldots, a_{q-1}) = \prod_{j=1}^{q} \left(\sum_{i=0}^{q-1} a_i \xi_q^{ij} \beta^i \right)$.
- If $y \in M$, where M is a finite extension of K, then we will say that "y is integral at $\mathfrak{p}_K$" if y is integral at every factor of $\mathfrak{p}_K$ in M.

We are now ready to state and prove the main technical proposition of this section.

Proposition 3.2. *Let $x \in F$. Let $M \subset F$ be a number field containing $K(x)$. Then*

$$N(a_0, \ldots, a_{q-1}) = h \tag{3.8}$$

has solutions $a_0, \ldots, a_{q-1} \in L_x = F(\beta(x))$ only if for all fields M as above, for all factors $\mathfrak{p}_M$ of $\mathfrak{p}_K$ in M, we have that

$$ord_{\mathfrak{p}_M} x > \frac{(-q+1) ord_{\mathfrak{p}_M}(g)}{r(s+1)}. \tag{3.9}$$

In the unramified case we can make a stronger statement: equation (3.8) has solutions $a_0, \ldots, a_{q-1} \in L_x = F(\beta_x)$ only if x is integral at every factor of $\mathfrak{p}_K$. (Note that (3.9) is automatically satisfied if x is integral at all the factors of $\mathfrak{p}_K$ in F.) Finally, if $x \in K$ and is integral at $\mathfrak{p}_K$, then (3.8) has solutions $a_0, \ldots, a_{q-1} \in K(\beta_x)$.

Proof. We start with the first part of the proposition concerning the necessary conditions for the existence of $a_0, \ldots, a_{q-1}$, that is suppose (3.8) has solutions as described in the statement of the proposition. We will first show that this part of the proposition holds for a particular class of fields M. We will consider two cases: $\beta(x) \in F$ and $\beta(x) \notin F$. In the first case let $M \supseteq K(x, \beta(x))$. If $\beta(x) \notin F$, then it is of degree q over F by Lemma 12.2, and for each i we can write

$$a_i = A_{i,0} + A_{i,1}\beta(x) + \ldots + A_{i,q-1}\beta(x)^{q-1},$$

where $A_{i,0}, \ldots, A_{i,q-1} \in F$. In this case, let $M \supseteq K(x, A_{0,0}, \ldots, A_{q-1,q-1})$. Then each $a_i \in M(\beta(x))$ and $[M(\beta(x)) : M] = q$.

Now assume that either we are in the unramified case and for some factor $\mathfrak{p}_M$ of $\mathfrak{p}_K$, we have that x is not integral at $\mathfrak{p}_M$, or (3.9) does not hold.

We begin with the unramified case. Let $\mathfrak{p}_M$ be an M-factor of $\mathfrak{p}_K$ such that $\mathrm{ord}_{\mathfrak{p}_M} x < 0$. Then since in the case under consideration we have that $\mathrm{ord}_{\mathfrak{p}_M} g = \mathrm{ord}_{\mathfrak{p}_K} g$, we conclude that $\mathrm{ord}_{\mathfrak{p}_M} h < 0$ and $\mathrm{ord}_{\mathfrak{p}_M} h \ncong 0 \mod q$. Thus, $h^{-1} + z^q \cong z^q \mod \mathfrak{p}_M$. Hence if the extension $M(\beta(x))/M$ is non-trivial, $\mathfrak{p}_M$ will split completely in this extension. Let $\mathfrak{p}_{M(\beta(x))}$ be any factor of $\mathfrak{p}_M$ in $M(\beta(x))$. Given the arguments above, whether $M(\beta(x)) = M$ or is a non-trivial extension of M, we have that $X^q - b$ is irreducible over the residue field of $\mathfrak{p}_{M(\beta(x))}$. Since $\mathfrak{p}_{M(\beta(x))}$ is prime to q and does not occur in the divisor of b, the irreducibility of $X^q - b$ over the residue field of $\mathfrak{p}_{M(\beta(x))}$ implies that $\mathfrak{p}_{M(\beta(x))}$ does not split in the extension $M(\beta(x), \beta)/M(\beta(x))$. Further,

$$\mathrm{ord}_{\mathfrak{p}_{M(\beta(x))}} h = \mathrm{ord}_{\mathfrak{p}_M} h = \mathrm{ord}_{\mathfrak{p}_K} h \ncong 0 \mod q.$$

Therefore, h cannot be a $M(\beta(x))$-norm of an element from $M(\beta, \beta(x))$. But (3.8) asserts precisely that. Consequently, we have a contradiction and conclude that in the unramified case, if for some $x \in F$ it is the case that (3.8) has solutions $a_0, \ldots, a_{q-1} \in M(\beta(x))$, then x is integral at $\mathfrak{p}_K$.

We will now drop the assumption that $\mathfrak{p}_K$ has no ramified factors in any finite extension of K contained in F. Define a field M as above and assume that (3.9) does not hold. Then, given our definition of h and our assumption on the ramification degrees, we still have $\mathrm{ord}_{\mathfrak{p}_M} h < 0$ and $\mathrm{ord}_{\mathfrak{p}_M} h \ncong 0 \mod q$ as above. Therefore from this point on we can proceed as before.

Now assume M' is an arbitrary subfield of F containing K. Let $x \in M'$ and suppose that equation (3.8) has solutions $a_0, \ldots, a_{p-1} \in L_x = F(\beta(x))$ as described above. Let $M = M'(x, \beta(x))$ or $M = M'(x, A_{0,0}, \ldots, A_{q-1,q-1})$ as above depending on whether $\beta(x) \in F$. Let $\mathfrak{p}_{M'}$ be the prime of M' below $\mathfrak{p}_M$. Then by the arguments above, depending on whether we are in the ramified or the unramified case, we have that either inequality (3.9) holds or $\mathrm{ord}_{\mathfrak{p}_M} x > 0$. Let e the ramification degree of $\mathfrak{p}_M$ over $\mathfrak{p}_{M'}$. Then we also have that either

$$\mathrm{ord}_{\mathfrak{p}_M} x > \frac{(-q+1)\mathrm{ord}_{\mathfrak{p}_M}(g)}{r(s+1)} \Rightarrow \frac{1}{e}\mathrm{ord}_{\mathfrak{p}_M} x > \frac{(-q+1)\mathrm{ord}_{\mathfrak{p}_M}(g)}{er(s+1)} \Rightarrow \mathrm{ord}_{\mathfrak{p}_{M'}} x > \frac{(-q+1)\mathrm{ord}_{\mathfrak{p}_{M'}}(g)}{r(s+1)},$$

or

$$\mathrm{ord}_{\mathfrak{p}_M} x > 0 \Rightarrow \mathrm{ord}_{\mathfrak{p}_{M'}} x > 0.$$

Now the second assertion of the proposition follows directly from Theorem 2.1 of [27]. □

Our next task is to reduce the number of assumptions on the field F necessary for the definability of integrality at a prime. This will be accomplished in the two lemmas below: one for the general case and one for the unramified case. We treat the general case first.

Lemma 3.3. *Let L be an algebraic, possibly infinite extension of $\mathbb{Q}$. Let Z be a number field contained in L such that L is normal over Z. Let $\mathfrak{p}_Z$ be a prime of Z and assume that the following conditions are satisfied.*

- *There exists a non-negative integer m_f such that any prime lying above $\mathfrak{p}_Z$ in a number field contained in L has a relative degree f over Z with $ord_q f \leq m_f$.*
- *There exists a non-negative integer m_e such that any prime lying above $\mathfrak{p}_Z$ in a number field contained in L has a ramification degree e over Z with $ord_q e \leq m_e$.*

Then there exists a finite extension K of Z such that K and $F = KL$ satisfy the assumptions in 3.1 for the general case with respect to all factors $\mathfrak{p}_K$ of $\mathfrak{p}_Z$ in K.

Proof. Let $\mathbf{M}_e$ be the set of all exponents m such that $e = e_0 q^m$ with $(e_0, q) = 1$ is a ramification degree over Z for a number field prime lying above $\mathfrak{p}_Z$. This is a set of non-negative integers bounded from above and therefore must have a maximal element $\bar{m}$. Let U_0 be a number field with a prime $\mathfrak{p}_{U_0}$ above $\mathfrak{p}_Z$ with the ramification degree over Z divisible by $q^{\bar{m}}$. Let U_e be the Galois closure of U_0 over Z and observe that U must also have a prime $\mathfrak{p}_{U_e}$ above $\mathfrak{p}_Z$ with the ramification degree over Z divisible by $q^{\bar{m}}$, since $e(\mathfrak{p}_{U_e}/\mathfrak{p}_Z) = e(\mathfrak{p}_{U_e}/\mathfrak{p}_{U_0})e(\mathfrak{p}_{U_0}/\mathfrak{p}_Z)$. Further, since U_e is Galois over Z, it is the case that for any U_e-prime $\mathfrak{q}_{U_e}$ above $\mathfrak{p}_Z$ we have that $\text{ord}_q e(\mathfrak{q}_{U_e}/\mathfrak{p}_Z) = \bar{m}$. Next we note that if $\bar{U}/U_e$ is a finite extension of number fields with $\bar{U} \subset L$ and $\mathfrak{p}_{\bar{U}}$ is a prime above $\mathfrak{p}_{U_e}$, then $\text{ord}_q e(\mathfrak{p}_{\bar{U}}/\mathfrak{p}_{U_e}) = 0$.

Similarly we can find a field U_f, Galois over Z, so that for any finite extension $\hat{U}$ of U_f and any prime $\mathfrak{p}_{\hat{U}}$ lying above $\mathfrak{p}_Z$ in $\hat{U}$ we have that $\text{ord}_q f(\mathfrak{p}_{\hat{U}}/\mathfrak{p}_{U_f}) = 0$. Let $U = U_e U_f$ (observe that U/Z is Galois), let $K = U(\xi_q)$ and let $F = KL = L(\xi_q)$. Note that F/Z is also a normal extension. Let N be a number field such that $K \subset N \subset F$. Let $\mathfrak{p}_U$ be any prime lying above above $\mathfrak{p}_Z$ in U, and let $\mathfrak{p}_N$ be any prime above $\mathfrak{p}_U$ in N. Let $B \in R(\mathfrak{p}_Z)$ (the residue field of $\mathfrak{p}_H$) be such that B is not a q-th power. We claim that B is not a q-th power in $R(\mathfrak{p}_N)$ and $e(\mathfrak{p}_N/\mathfrak{p}_U) \not\equiv 0 \mod q$.

Indeed, since $N \subset L(\xi_q)$, for some field T such that $U \subset T \subset L$ we have that $N \subset T(\xi_q)$. Without loss of generality we can assume that $N = T(\xi_q)$. Let $\mathfrak{p}_T$ be a prime above $\mathfrak{p}_Z$ in T. Then, by construction of U, we know that $e(\mathfrak{p}_T/\mathfrak{p}_U) \not\equiv 0 \mod q$ and $f(\mathfrak{p}_T/\mathfrak{p}_U) \not\equiv 0 \mod q$. Next we observe that $e(\mathfrak{p}_N/\mathfrak{p}_T)$ and $f(\mathfrak{p}_N/\mathfrak{p}_T)$ are both divisors of $q-1$ and therefore are not divisible by q, so that $e(\mathfrak{p}_N/\mathfrak{p}_U) \not\equiv 0 \mod q$ and $f(\mathfrak{p}_N/\mathfrak{p}_U) \not\equiv 0 \mod q$. Consequently, we also have $e(\mathfrak{p}_N/\mathfrak{p}_K) \not\equiv 0 \mod q$ and $f(\mathfrak{p}_N/\mathfrak{p}_K) \not\equiv 0 \mod q$. Further, since $([R(\mathfrak{p}_N) : R(\mathfrak{p}_U)], q) = 1$, we also conclude that B is not a q-th power in $R(\mathfrak{p}_N)$. □

We now consider the unramified case.

Lemma 3.4. *Let L be an algebraic, possibly infinite extension of $\mathbb{Q}$. Let Z be a number field contained in L such that L is normal over Z. Let $\mathfrak{p}_Z$ be a prime of Z and assume that the following conditions are satisfied.*

- *There exists a non-negative integer m_f such that any prime lying above $\mathfrak{p}_Z$ in a number field contained in L has a relative degree f over Z with $ord_q f \leq m_f$.*
- *There exists a non-negative integer m_e such that any prime lying above $\mathfrak{p}_Z$ in a number field contained in L has a ramification degree e over Z with $e \leq m_e$.*

Then there exists a finite extension K of Z such that K and $F = KL$ satisfy the assumptions in 3.1 for the unramified case with respect to all factors $\mathfrak{p}_K$ of $\mathfrak{p}_Z$ in K.

Proof. The proof of this lemma is almost identical to the proof of Lemma 3.3. The only difference will come in the way the field U_e is selected. First we will let $\mathbf{M}_e$ be the set of all non-negative integers e such that e is a ramification degree for a prime lying above $\mathfrak{p}_Z$ in some number field contained in L. The set $\mathbf{M}_e$, as in Lemma 3.3, will have a maximal element $\bar{e}$. Let U_e be a finite Galois extension of Z contained in L such that for some U_e-prime $\mathfrak{p}_U$ lying above $\mathfrak{p}_Z$ the ramification degree over Z is $\bar{e}$. From this point on the proof proceeds as in Lemma 3.3. □

Remark 3.5. From the proof of the lemmas it is clear that if a field $Z \subset L$ and a Z-prime $\mathfrak{p}_Z$ satisfy the assumptions of Lemmas 3.3 or 3.4, then any finite extension T of Z and any T-prime lying above $\mathfrak{p}_Z$ will also satisfy the requirements of Lemmas 3.3 or 3.4 respectively.

Finally we state the main results of this section. As above we separate out the general and the unramified case for readability. We start with a general case again.

Theorem 3.6. *Let $L, Z, \mathfrak{p}_Z, q$ be as in Lemma 3.3. Then there exist an element $u \in L$ and a subset $\mathscr{X}$ of L satisfying the following conditions:*

- *If $x \in \mathscr{X}$, then ux is integral with respect to $\mathfrak{p}_Z$.*
- *If $x \in Z$ and x is integral at $\mathfrak{p}_Z$, then $x \in \mathscr{X}$.*
- *$\mathscr{X}$ is Diophantine over L.*

Proof. Let F and K be as in Lemma 3.3 . For each factor $\mathfrak{p}_K$ of $\mathfrak{p}_Z$ in K, let $g = g(\mathfrak{p}_K) \in K$ be defined as in Notation and Assumptions 3.1 with respect to $\mathfrak{p}_K$. Then by Proposition 3.2, and since intersection of Diophantine sets is Diophantine, there exists a set $\mathscr{Y} \subset F$ satisfying the following conditions.

- If $y \in \mathscr{Y}$, then $\left(\prod_{\mathfrak{p}_K|\mathfrak{p}_T} g(\mathfrak{p}_K)^q\right) y$ is integral with respect to $\mathfrak{p}_Z$.
- If $y \in K$ and y is integral at every $\mathfrak{p}_K$ above $\mathfrak{p}_Z$, then $y \in \mathscr{Y}$.
- $\mathscr{Y}$ is Diophantine over F.

Let $\mathscr{X} = \mathscr{Y} \cap L$. Then $\mathscr{X}$ is Diophantine over L by Proposition 2.6. Next let $u \in T$ be such that $\mathrm{ord}_{\mathfrak{p}_Z} u \geq \mathrm{ord}_{\mathfrak{p}_K} g(\mathfrak{p}_K)^q$ for all factors of $\mathfrak{p}_z$ in K. Now observe that if $x \in \mathscr{X}$ then $x \in \mathscr{Y}$ and ux is integral at $\mathfrak{p}_Z$. Conversely, if $x \in Z$ and is integral at $\mathfrak{p}_Z$, then $x \in K$ and is integral at every factor of $\mathfrak{p}_Z$ in K. Thus $x \in \mathscr{Y} \cap L = \mathscr{X}$. □

We now proceed to the unramified case.

Theorem 3.7. *Let $L, Z, \mathfrak{p}_Z, q$ be as in Lemma 3.4. Then there exists a subset $\mathscr{X}$ of L satisfying the following conditions:*

- *If $x \in \mathscr{X}$, then x is integral with respect to $\mathfrak{p}_Z$.*
- *If $x \in Z$ and x is integral at $\mathfrak{p}_Z$, then $x \in \mathscr{X}$.*
- *$\mathscr{X}$ is Diophantine over L.*

Proof. The proof is completely analogous to the proof of Theorem 3.6 but relies on Lemma 3.4 and the unramified case of Proposition 3.2. □

We finish this section with a corollary which we will use for the cases of infinite cyclotomic and abelian equations.

Corollary 3.8. *Suppose L is a normal, algebraic, possibly infinite extension of $\mathbb{Q}$ such that for some rational prime q for every number field M contained in L we have that $[M : \mathbb{Q}] \not\equiv 0 \mod q$. Then any number field $M \subset L$ and any M-prime $\mathfrak{p}_M$ satisfy the assumptions of Theorem 3.6 or Theorem 3.7.*

Proof. Let $M \subset L$ be a number field. Let M' be a finite extension of M. Without loss of generality we can assume that M' is Galois over $\mathbb{Q}$. Then for any prime $\mathfrak{q}_{M'}$ of M' we have that $e(\mathfrak{q}_{M'}/\mathfrak{q}_{\mathbb{Q}}) f(\mathfrak{q}_{M'}/\mathfrak{q}_{\mathbb{Q}}) | [M' : \mathbb{Q}]$, where $\mathfrak{q}_{\mathbb{Q}}$ is the rational prime below $\mathfrak{q}_{M'}$. Thus, $e(\mathfrak{q}_{M'}/\mathfrak{q}_{\mathbb{Q}}) f(\mathfrak{q}_{M'}/\mathfrak{q}_{\mathbb{Q}}) \not\equiv 0 \mod q$. Let $\mathfrak{p}_M$ be any prime of M and let $\mathfrak{p}_{M'}$ be a prime of M' above it. Then

$$e(\mathfrak{p}_{M'}/\mathfrak{p}_M) = \frac{e(\mathfrak{p}_{M'}/\mathfrak{p}_{\mathbb{Q}})}{e(\mathfrak{p}_M/\mathfrak{p}_{\mathbb{Q}})} \not\equiv 0 \mod q.$$

Similarly,

$$f(\mathfrak{p}_{M'}/\mathfrak{p}_M) = \frac{f(\mathfrak{p}_{M'}/\mathfrak{p}_{\mathbb{Q}})}{f(\mathfrak{p}_M/\mathfrak{p}_{\mathbb{Q}})} \not\equiv 0 \mod q.$$

□

We now introduce the following notation.

Notation 3.9. Let K be a number field, let F be an algebraic possibly infinite extension of K, and let $\mathscr{C}_K$ be a finite set of primes of K. Then let $I_{\mathscr{C}_K/F}(x, t_1, \ldots, t_k) \in K[x, t_1, \ldots, t_k]$ be such that

$$I_{\mathscr{C}_K/F}(x, t_1, \ldots, t_k) = 0 \tag{3.10}$$

has solutions in F only if $u_{\mathscr{C}_K/F} x$ is integral at all the primes of $\mathscr{C}_K$, where $u_{\mathscr{C}_K/F} \in \mathbb{Z}_{>0}$ is fixed and depends only $\mathscr{C}_K$. (As we have seen $u_{\mathscr{C}_K/F}$ can be equal to 1 in some cases.) Conversely, if $x \in K$ and is integral at all the primes of $\mathscr{C}_K$, then (3.10) has solutions in K.

4. **Norm Equations over Totally Real Fields: an Update.**

In this section we generalize the results from Section 3 of [30]. The main reason for this generalization is to allow for the treatment of arbitrary rings of $\mathscr{S}$-integers of infinite abelian extensions of $\mathbb{Q}$. We will point out the nature of the generalization below.

Notation and Assumptions 4.1. We start with a new set of assumptions and notation.

- Let M be a totally real number field of degree n over $\mathbb{Q}$.
- Let K be a subfield of M.
- Let L be a totally complex extension of degree 2 of K such that LM has no non-real roots of unity.
- Let $E_1/K, E_2/K$ be totally real cyclic extensions of odd prime degrees p_1 and p_2 respectively with $(p_i, [M_G : \mathbb{Q}]) = 1$ for $i = 1, 2$, where M_G is the Galois closure of M over $\mathbb{Q}$.
- If F is any number field, then let U_F denote the group of its integral units and let $\mathscr{P}(F)$ denote the set of all non-archimedean primes of F.
- Let N be any finite extension of a number field U. Let $\mathscr{T}_U$ (or $\mathscr{V}_U$, $\mathscr{W}_U$, $\mathscr{S}_U$, $\mathscr{E}_U$, $\mathscr{N}_U$, $\mathscr{L}_U$, $\mathscr{R}_U$, ...) be any set of primes of U. Then let $\mathscr{T}_N$ (or $\mathscr{V}_N$, $\mathscr{W}_N$, $\mathscr{S}_N$, $\mathscr{E}_N$, $\mathscr{N}_N$, $\mathscr{L}_N$, $\mathscr{R}_N$, ...) be the set of primes of N lying above the primes of $\mathscr{T}_U$. Also let $\overline{\mathscr{T}_N}$ be the closure of $\mathscr{T}_N$ in $\mathscr{P}(N)$ with respect to conjugation over $\mathbb{Q}$.
- Let $\mathscr{V}_K$ be a set of primes of K not splitting in either of the extensions E_i/K, $i = 1, 2$.
- Let $\mathscr{S}_K = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\} \subset \mathscr{P}(K)$ be a set of primes not splitting in the extensions M/K and E_2/K. Assume that at least one prime in $\mathscr{S}_K$ splits completely in the extension E_1L/K.
- Let $\mathscr{W}_K = \mathscr{V}_K \cup \mathscr{S}_K$.
- Let h_{LE_1} be a class number of LE_1.

Below we prove a generalization of Lemma 3.1 of [30]. The main difference between the old and the new versions of the lemma is that we replace a single K-prime $\mathfrak{p}$ splitting in the extension LE_1/K and remaining prime in the extension M/K with a finite set of primes satisfying the same conditions.

Lemma 4.2. *Let $x \in O_{MLE_1, \mathscr{W}_{MLE_1}}$ be a solution to the following system of equations.*

$$\begin{cases} \mathbf{N}_{MLE_1/ML}(x) = 1 \\ \mathbf{N}_{MLE_1/E_1M}(x) = 1 \end{cases} \tag{4.1}$$

Then $x^{2h_{LE_1}} \in E_1L$. Further such a solution exists.

Proof. First of all note that no prime of $\mathscr{W}_M \setminus \mathscr{S}_M$, splits in the extension ME_1/M by Lemmas 12.4 and 12.6. Further, we note that given our assumptions on $\mathscr{S}_K$, by Lemma 12.6, all primes of $\mathscr{S}_M$ split completely in the extension MLE_1/M.

Suppose now that $x \in LE_1M$ is a solution to the system of norm equations. Then the divisor of x must be composed of the primes lying above primes of E_1M and LM splitting in the extensions LE_1M/E_1M and LE_1M/LM respectively. Given the fact that both extensions are cyclic of distinct prime degrees, we can conclude that LE_1M-primes occurring in the divisor of x lie above M-primes splitting completely in the extension LE_1M/M. Thus, if $x \in O_{MLE_1, \mathscr{W}_{MLE_1}}$ is a solution to the norm system, its divisor consists of MLE_1-factors of primes in $\mathscr{S}_M$ only. Further, since LE_1M/E_1M is a totally complex extension of degree 2 of a totally real field, all the integral solutions to the second equation have to be roots of unity. Since ME_1L does not have any complex roots of unity, we can conclude the following. Let x_1, x_2 be two solutions to the second norm equation above such that x_1 and x_2 have the same divisor. Then on the one hand, $x_1 = \pm x_2$. On the other hand, since primes of $\mathscr{S}_K$ do not split in the extension M/K and primes of $\mathscr{S}_K$ split completely in the extension LE_1/K, we know that LE_1-factors of primes in $\mathscr{S}_K$ do not split in the extension MLE_1/LE_1 by Lemma 12.5. Thus, there exists $y \in O_{LE_1, \mathscr{W}_{LE_1}}$ such that y has the same divisor as $x^{h_{LE_1}}$. Therefore, $y = \nu x^{h_{E_1L}}$, where ν is an integral unit of MLE_1, and $\mathbf{N}_{ME_1L/E_1M}(y) = \mu$ is an integral unit of E_1M. On the other hand, since $[E_1L : E_1] = [LE_1M : E_1M] = 2$, we have that $\mathbf{N}_{ME_1L/E_1M}(y) = \mathbf{N}_{E_1L/E_1}(y)$ and therefore μ is an integral unit of E_1. Let $\bar{y} = \mu^{-1}y^2$. Then $\mathbf{N}_{ME_1L/E_1M}(\bar{y}) = \mathbf{N}_{E_1L/E_1}(\bar{y}) = 1$. The divisors of $\bar{y}$ and $x^{2h_{E_1L}}$ are the same and therefore $x^{2h_{E_1L}} \in E_1L$.

The proof of the fact that the system always has solutions in $O_{LE_1, \mathscr{W}_{LE_1}}$ which are not roots of unity remains the same as in Lemma 3.1 of [30].

□

5. **Norm Equations and Extensions of Degree 2 Real Fields.**

In this section we revisit a result of Denef and Lipshitz from [8] and show that under some assumptions it has a version that holds in the infinite extensions too. We will also prove a version of this result for "large" rings. We start with a notation and assumptions list and some facts about the primes and norm equations in the extensions under consideration.

Notation and Assumptions 5.1. Below we use Notation and Assumptions 4.1 as well as the following notation and assumptions.

- Let G be an extension of degree 2 of K generated by $\alpha \in O_G$ with $\alpha^2 = a \in O_K$.
- Let H be an extension of degree 2 of K generated by $\delta \in O_H$ such that $\delta^2 = d \in O_K$.
- For all embeddings $\sigma : K \longrightarrow \mathbb{C}$, assume that $\sigma(d) > 0$ if and only if $\sigma(a) < 0$. Further, assume that $|\sigma(a)| > 1$ for all σ's as above.
- For any number field N, let r_N be the number of real embeddings of N into $\tilde{\mathbb{Q}}$, and let $2s_N$ be the number of non-real embeddings of N into $\tilde{\mathbb{Q}}$.
- Assume $s_G > 0$.
- Let $\mathscr{Z}_K$ be a set of primes of K not splitting in the extension E_2/K. We will assume that $\mathscr{Z}_K \supseteq \mathscr{W}_K$.

Lemma 5.2. *There exists $\varepsilon \in O_{HGE_2}$ such that ε is not a root of unity, and*

$$\begin{cases} \mathbf{N}_{HGE_2M/E_2GM}(\varepsilon) = 1, \\ \mathbf{N}_{GHE_2M/HGM}(\varepsilon) = 1. \end{cases} \tag{5.1}$$

Proof. Since $[M : \mathbb{Q}] = n$, we have that $[GM : \mathbb{Q}] = 2n$, $[GHM : \mathbb{Q}] = 4n$, $[HGME_2 : \mathbb{Q}] = 4p_2n$, and $[E_2GM : \mathbb{Q}] = 2p_2n$. Next we note that given a number field extension U/F, the integral solutions to the equation $\mathbf{N}_{U/F}(x) = 1$ in U form a multiplicative group whose rank is equal to the difference of ranks between the integral unit groups of U and F. Let

$$A_{GM} = \{x \in O_{HGME_2} : \mathbf{N}_{HGME_2/GM}(x) = 1\},$$
$$A_{GMH} = \{x \in O_{HGME_2} : \mathbf{N}_{HGME_2/GMH}(x) = 1\},$$
$$A_{E_2GM} = \{x \in O_{HGME_2} : \mathbf{N}_{HGME_2/E_2GM}(x) = 1\},$$

It is clear that $A_{GMH} \cup A_{E_2GM} \subseteq A_{GM}$. By computing the ranks of the integral unit groups involved we will show that

$$\text{rank}A_{GMH} + \text{rank}A_{E_2GM} > \text{rank}A_{GM}. \tag{5.2}$$

This inequality implies that $A_{GMH} \cap A_{E_2GM}$ contains an element of infinite order. First of all, we have that

$$r_{GM} + 2s_{GM} = 2n.$$

Further by Dirichlet Unit Theorem we know that

$$\text{rank}U_{GM} = r_{GM} + s_{GM} - 1.$$

Given our assumptions (see Notation and Assumptions 5.1) on HM and GM, every real embedding of GM will extend to two non-real embeddings of GMH. (Non-real embeddings obviously always extend to non-real embeddings.) Thus, GMH will have no real embeddings and $4n$ non-real embeddings into $\tilde{\mathbb{Q}}$. Therefore,

$$\text{rank}U_{GMH} = 2n - 1 = r_{GM} + 2s_{GM} - 1.$$

Since E_2 is a totally real field, GME_2 has p_2r_{GM} real embeddings and $2p_2s_{GM}$ non-real embeddings with

$$\text{rank}U_{E_2GM} = p_2r_{GM} + p_2s_{GM} - 1.$$

Finally, adjoining E_2 to GMH will result in the field with $4p_2n$ non-real embeddings so that

$$\text{rank}U_{GMHE_2} = 2p_2n - 1 = p_2r_{GM} + 2p_2s_{GM} - 1.$$

To show that (5.2) holds note the following:

$$\text{rank}A_{GM} = \text{rank}U_{HGME_2} - \text{rank}U_{GM} = p_2r_{GM} + 2p_2s_{GM} - r_{GM} - s_{GM},$$
$$\text{rank}A_{GMH} = \text{rank}U_{HGME_2} - \text{rank}U_{GMH} = p_2r_{GM} + 2p_2s_{GM} - r_{GM} - 2s_{GM},$$
$$\text{rank}A_{E_2GM} = \text{rank}U_{HGME_2} - \text{rank}U_{E_2GM} = p_2r_{GM} + 2p_2s_{GM} - p_2r_{GM} - p_2s_{GM} = p_2s_{GM},$$

Thus,

$\text{rank}A_{GMH} + \text{rank}A_{E_2GM} = p_2 r_{GM} + 3p_2 s_{GM} - r_{GM} - 2s_{GM} > p_2 r_{GM} + 2p_2 s_{GM} - r_{GM} - s_{GM} = \text{rank}A_{GM}$,

as long as $p_2 s_{GM} > s_{GM}$. This last inequality obviously holds for any $p_2 > 1$ since we assumed that $s_{GM} \geq 1$. □

The next lemma will state an easy result which will be crucial in eliminating the unwanted primes in the denominator.

Lemma 5.3. *The primes in $\mathscr{Z}_{GMH}$ do not split in the extension $GMHE_2/GMH$.*

Proof. This lemma follows from the fact that $([E_2 : K], [GMH : K]) = 1$ and Lemma 12.4. □

Corollary 5.4. *Let m be divisible by the size of the group of roots of unity in $GMHE_2$. Then for any $\varepsilon \in O_{GMHE_2, \mathscr{Z}_{GMHE_2}}$ such that it is a solution to (5.1) we have that $\varepsilon^m \in O_{MHE_2}$. Further, if we assume that all the roots of unity in $GMHE_2$ are already in GM, we can replace m by 2.*

Proof. First, since $\varepsilon \in O_{GMHE_2, \mathscr{W}_{GMHE_2}}$, the only primes which can occur in the denominator of the divisor of ε are primes from $\mathscr{W}_{GMHE_2}$. Secondly, since $\mathbf{N}_{GME_2H/HGM}(\varepsilon) = 1$, the only primes which can occur in the numerator of the divisor of ε are the primes that have a distinct conjugate over GMH which is allowed in the denominator of the divisors of the elements of $O_{GMHE_2, \mathscr{W}_{GMHE_2}}$. But by Lemma 5.3, no primes of $\mathscr{W}_{GMHE_2}$ has a distinct conjugate over GMH. Consequently, ε has a a trivial divisor and therefore is an integral unit.

Second, let

$$A_{E_2M} = \{x \in O_{HE_2M} : \mathbf{N}_{HE_2M/E_2M}(x) = 1\},$$

and note that $A_{E_2M} \subseteq A_{E_2GM}$ since GM and HM are linearly disjoint over E_2M by assumptions in 5.1. Using notation from Lemma 5.2, we have that $\text{rank}A_{E_2GM} = p_2 s_{GM}$. To compute the rank of A_{E_2M} we need to compute the ranks of integral unit groups of HE_2M and E_2M. It is easy to see that

$$\text{rank}U_{E_2M} = p_2 n - 1 = p_2 \frac{r_{GM} + 2s_{GM}}{2} - 1 = \frac{p r_{GM}}{2} + p s_{GM} - 1.$$

To compute, U_{HE_2M} we can look at the number of real and non-real embeddings of HM first and then multiply these numbers by p_2 to get the analogous information for E_2HM. From the assumptions in 5.1 we have that HM has $2s_{GM}$ real and r_{GM} non-real embeddings into $\tilde{\mathbb{Q}}$. Thus E_2HM has $2p_2 s_{GM}$ real and $p_2 r_{GM}$ non-real embeddings. Therefore,

$$\text{rank}U_{HE_2M} = 2p_2 s_{GM} + \frac{p_2 r_{GM}}{2} - 1.$$

Hence, $\text{rank}A_{E_2M} = p_2 s_{GM} = \text{rank}A_{E_2GM}$. Now suppose $\varepsilon \in A_{E_2GM}$. Since the ranks are the same and $A_{E_2M} \subseteq A_{E_2GM}$, we conclude that for some positive $l \in \mathbb{N}$ we have that $\varepsilon^l \in O_{HE_2M}$. Let ε' be the conjugate of ε over E_2HM. Then, $(\varepsilon/\varepsilon')^l = 1$ or, in other words, $\varepsilon/\varepsilon' = \xi$ – a root of unity in $GMHE_2$ with $\mathbf{N}_{GMHE_2/GME_2}(\xi) = 1$. Thus $l|m$. If we now assume that $\xi \in GM$, we conclude that $\mathbf{N}_{GMHE_2/GME_2}(\xi) = \xi^2 = 1$. Thus, $\varepsilon' = \pm\varepsilon$ and therefore $\varepsilon^2 \in HE_2M$. □

6. **Bounds for Extensions of Degree 2.**

Notation 6.1. We now add to the list of Notation and Assumptions 4.1 and 5.1.

- Assume that an integral unit μ generates E_2 over K. Denote the monic irreducible polynomial of μ over K by $P(X)$, and assume that $P(X) \in \mathbb{Z}[X]$. (This assumption implies that μ is of degree p_2 over $\mathbb{Q}$, K, M and GM.)
- Let $\mathscr{M}_{GM} \subset \mathscr{Z}_{GM}$ be a set of GM-primes lying above M-primes not splitting in the extension GM/M.
- Let $\mathscr{U}_{GM} = \mathscr{M}_{GM} \cup \mathscr{S}_{GM}$.
- Let $\mathscr{E}_K$ contain all the primes $\mathfrak{p}$ of $\mathscr{Z}_K$ such that $\mathfrak{p}$ divides the discriminant of $P(X)$ and all the primes of $\mathscr{S}_K$. Given our definition of $\mathscr{Z}_K$, we have that $\mathscr{E}_K$ is a finite set of K-primes. (In the future we might add primes to this set, but it will always remain finite.) Let $N_{\mathscr{E}}$ be a positive integer divisible by all the primes of $\mathscr{E}_K$.
- Let $Q(X) = P(N_{\mathscr{E}_K} X)$.

Eventually we will use $P(X)$ to get away from the factors of primes in $\mathscr{Z}_K$ in the denominator. We know that for all primes $\mathfrak{p} \in \mathscr{Z}_K$ not dividing the discriminant of $P(X)$, for all $x \in K$, it is the case that $\mathrm{ord}_{\mathfrak{p}} P(x) \leq 0$. However we need to take care of the finitely many extra primes in $\mathscr{E}_K$ possibly dividing the discriminant of $P(X)$ or inconvenient in some other ways (as will be explained later). To that effect we adjust $P(X)$.

Lemma 6.2. *Let $x \in GM$ and assume that x is integral at all the primes of $\overline{\mathscr{E}}_{GM}$. Then for all $\mathfrak{p} \in \overline{\mathscr{Z}}_{GM}$ we have that $ord_{\mathfrak{p}} P(N_{\mathscr{E}} x) \leq 0$. Further, for all $\mathfrak{p} \in \overline{\mathscr{E}}_{GM}$ we have that $ord_{\mathfrak{p}} P(N_{\mathscr{E}} x) = 0$.*

Proof. Let C be the Galois closure of GM over $\mathbb{Q}$. It is enough to show that the lemma holds for C in place of GM and for $\mathscr{Z}_C$ and $\mathscr{E}_C$ in place of $\mathscr{Z}_{GM}$ and $\mathscr{E}_{GM}$ respectively. First observe that $[C : \mathbb{Q}] = [M_G : \mathbb{Q}]2^j$, for some $j \in \mathbb{Z}_{>0}$. Thus, given our assumption that p_2 is odd and $([M_G : \mathbb{Q}], p_2) = 1$, we conclude that $([C : K], p_2) = 1$. Second, by Lemma 12.5, no prime of $\mathscr{Z}_C$ will split in the extension CE_2/C. Suppose for some $\mathfrak{p} \in \mathscr{Z}_C \setminus \mathscr{E}_C$, some $x \in C$ we have that $\mathrm{ord}_{\mathfrak{p}} Q(X) > 0$. Then $P(X)$ has a root modulo $\mathfrak{p}$. But then $\mathfrak{p}$ has a relative degree one factor in the extension CE_2/C (see [9], page 25), contradicting our arguments above. Suppose now that $\mathfrak{p} \in \mathscr{E}_C$, $x \in C$ is integral at $\mathfrak{p}$ and $Q(x) = P(N_{\mathscr{E}} x) \cong 0 \mod \mathfrak{p}$. But given our assumption on x and $N_{\mathscr{E}}$ we have that $N_{\mathscr{E}} x \cong 0 \mod \mathfrak{p}$ and the free term of $P(X)$ is an integral unit. Hence we have a contradiction. Finally, suppose that $\bar{\mathfrak{q}}$ is a conjugate of $\mathfrak{q} \in \mathscr{Z}_C$ over $\mathbb{Q}$, and for some $\bar{x} \in C$ we have that $\mathrm{ord}_{\bar{\mathfrak{q}}} Q(\bar{x}) > 0$. Then, since $Q(T) \in \mathbb{Z}[T]$, we have that $\mathrm{ord}_{\mathfrak{q}} Q(x) > 0$.

Suppose now that $\mathfrak{p} \in \overline{\mathscr{E}}_C$. By the argument above we have that $\mathrm{ord}_{\mathfrak{p}} P(N_{\mathscr{E}} x) \leq 0$. On the other hand, $N_{\mathscr{E}} x$ is, by assumption, integral at $\mathfrak{p}$, and $P(X) \in \mathbb{Z}[X]$. Thus, $P(N_{\mathscr{E}} x)$ is also integral at $\mathfrak{p}$. Consequently, $P(N_{\mathscr{E}} x)$ is a unit at $\mathfrak{p}$. □

Notation and Assumptions 6.3. Here we make additions to our notation set.

- Let $\beta_1, \ldots, \beta_{p_2}$ be all the roots of the polynomial $P(X)$.

We continue with a series of lemmas often used to obtain bounds on non-archimedean valuations.

Lemma 6.4. *Primes of $\mathscr{M}_{GME_2}$ lie above primes of M not splitting in the extension E_2GM/M.*

Proof. Since $([M : K], [GE_2 : K]) = 1$, the assertion of the lemma follows from Lemma 12.4. □

Lemma 6.5. *Let $x \in O_{GME_2, \mathscr{U}_{GME_2}}$, $x = y_0 + y_1\alpha \equiv 0 \mod \mathfrak{Z}$ in $O_{GME_2, \mathscr{U}_{GME_2}}$, where $y_0, y_1 \in E_2M$, $\mathfrak{Z}$ is an integral divisor of E_2M without any factors in $\mathscr{U}_{GME_2}$. (We remind the reader that α which has been defined in Notation and Assumptions 5.1 is an integral generator of GM over M.) Assume additionally that for any $\mathfrak{t} \in \overline{\mathscr{U}}_{GME_2}$ we have that $ord_{\mathfrak{t}} x \leq 0$ and x is a unit at all the primes of $\overline{\mathscr{S}}_{GME_2}$. Let $\mathbf{N}_{E_2GM/\mathbb{Q}}(x) = \frac{X}{Y}$, where $X, Y \in \mathbb{Z}$ and $(X, Y) = 1$ in $\mathbb{Z}$. Let $Z = \mathbf{N}_{E_2GM/\mathbb{Q}}(\mathfrak{Z})$. Then $\frac{Y}{Z}\mathbf{N}_{GME_2/\mathbb{Q}}(2\alpha y_1)$ is an integer.*

Proof. Let $\bar{x} = y_0 - y_1\alpha$ be the conjugate of x over E_2M. By assumption on $\mathscr{S}_{GME_2}$ we have that $\mathrm{ord}_{\mathfrak{p}} x = 0$ for all $\mathfrak{p} \in \mathscr{S}_{GME_2}$. Also, by assumption on $\mathscr{M}_{GME_2}$, for every $\mathfrak{t} \in \mathscr{M}_{GME_2}$ we have that

$$\mathrm{ord}_{\mathfrak{t}} x = \mathrm{ord}_{\mathfrak{t}} \bar{x}.$$

Thus, we have that

$$\mathrm{ord}_{\mathfrak{t}} 2\alpha y_1 = \mathrm{ord}_{\mathfrak{t}}(x - \bar{x}) \geq \mathrm{ord}_{\mathfrak{t}} x.$$

Since x does not have positive order at any prime of $\overline{\mathscr{U}}_{GME_2}$, the last inequality also asserts that

$$|\mathrm{ord}_{\mathfrak{t}} 2\alpha y_1| \leq |\mathrm{ord}_{\mathfrak{t}} x|.$$

Let $\frac{\mathfrak{B}}{\mathfrak{C}}$ be the GME_2-divisor of $2\alpha y_1$ with $\mathfrak{B}, \mathfrak{C}$ being relatively prime integral divisors such that all the factors of $\mathfrak{C}$ are in $\mathscr{M}_{GME}$. Let $\mathbf{N}_{GME_2/\mathbb{Q}}(2\alpha y_1) = \frac{B}{C}$, where $B, C \in \mathbb{Z}$ and are relatively prime in $\mathbb{Z}$. Then $C \Big| \mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{C})$ in $\mathbb{Z}$. Next, let $\frac{\mathfrak{X}}{\mathfrak{Y}}$, where $\mathfrak{X}, \mathfrak{Y}$ are relatively prime integral divisors with all the factors of $\mathfrak{Y}$ in $\mathscr{M}_{GME_2}$ and no factor of $\mathfrak{X}$ is in $\overline{\mathscr{M}}_{GME_2}$, be the GME_2-divisor of x. Given our assumptions on $\mathfrak{X}$ and $\mathfrak{Y}$, we can conclude that $\mathbf{N}_{GME/\mathbb{Q}}(\mathfrak{X})$ and $\mathbf{N}_{GME/\mathbb{Q}}(\mathfrak{Y})$ are relatively prime and therefore the divisor of Y is $\mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{Y})$. We claim that $\mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{C}) \Big| \mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{Y})$. Let

$$\mathfrak{C} = \prod_{\mathfrak{p} \in \mathscr{U}_{GME_2}} \mathfrak{p}^{a(\mathfrak{p})}, \tag{6.1}$$

$$\mathfrak{Y} = \prod_{\mathfrak{p} \in \mathscr{U}_{GME_2}} \mathfrak{p}^{b(\mathfrak{p})}, \tag{6.2}$$

where $a(\mathfrak{p}) = b(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$. Further, by the argument above, we also have that $b(\mathfrak{p}) \geq a(\mathfrak{p})$ for all $\mathfrak{p} \in \mathscr{U}_{GME_2}$. Using (6.1) and (6.2), we can write

$$\mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{C}) = \prod_{\mathfrak{p} \in \mathscr{U}_{GME_2}} p(\mathfrak{p})^{a(\mathfrak{p})f(\mathfrak{p})},$$

$$Y = \mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{Y}) = \prod_{\mathfrak{p} \in \mathscr{U}_{GME_2}} p(\mathfrak{p})^{b(\mathfrak{p})f(\mathfrak{p})},$$

where $p(\mathfrak{p})$ is the rational prime below a GME_2-prime $\mathfrak{p}$, and $f(\mathfrak{p})$ is the relative degree of $\mathfrak{p}$ over $\mathbb{Q}$. Now assertion follows from the fact that $b(\mathfrak{p}) \geq a(\mathfrak{p})$.

Next we note that for any $\mathfrak{q}$ such that $\mathrm{ord}_{\mathfrak{q}}\mathfrak{Z} > 0$ we have that $\mathrm{ord}_{\mathfrak{q}} 2\alpha y_1 \geq \mathrm{ord}_{\mathfrak{q}}\mathfrak{Z}$. This follows from the fact that $x \cong \bar{x} \equiv 0 \mod \mathfrak{Z}$, when we consider $\mathfrak{Z}$ as an ideal of $O_{GME_2,\mathscr{M}_{GME_2}}$. Since no prime factor of $\mathfrak{Z}$ is allowed in the denominator of the elements of our ring, we have that $Z \Big| B$ in $\mathbb{Z}$, and the lemma holds. $\square$

In the next lemma we remove the assumption that the primes allowed in the denominator stay prime in the extension GME_2/GM.

Lemma 6.6. *Let $x \in O_{GME_2,\mathscr{Z}_{GME_2}}, x = y_0 + y_1\alpha \equiv 0 \mod \mathfrak{Z}$ in $O_{GME_2,\mathscr{W}_{GME_2}}$, where $\mathfrak{Z}$ is an integral divisor, $ord_{\mathfrak{t}}\mathfrak{Z} = 0$ for all $\mathfrak{t} \in \mathscr{Z}_{GME_2}$. Assume additionally that for any $\mathfrak{t} \in \overline{\mathscr{Z}}_{GME_2}$ we have that $ord_{\mathfrak{t}}x \leq 0$. Let $\mathbf{N}_{E_2GM/\mathbb{Q}}(x) = \frac{X}{Y}$, where $X, Y \in \mathbb{N}$ and $(X, Y) = 1$ in $\mathbb{Z}$. Let $Z = \mathbf{N}_{E_2GM/\mathbb{Q}}(\mathfrak{Z})$. Then $\frac{Y^2}{Z}\mathbf{N}_{GME_2/\mathbb{Q}}(2\alpha y_1)$ is an integer.*

Proof. First of all, as above, we have that $2\alpha y_1 = x - \bar{x}$, where $\bar{x}$ is the conjugate of x over E_2. Therefore, given our assumptions, for any prime $\mathfrak{t} \in \mathscr{Z}_{GME_2}$, if $\mathrm{ord}_{\mathfrak{t}}(2\alpha y_1) < 0$, then $\mathrm{ord}_{\mathfrak{t}}x < 0$ or $\mathrm{ord}_{\mathfrak{t}}\bar{x} < 0$. Thus, we need to consider three cases:

$$r(\mathfrak{t}) = \mathrm{ord}_{\mathfrak{t}}x = \mathrm{ord}_{\mathfrak{t}}\bar{x},$$
$$r_1(\mathfrak{t}) = \mathrm{ord}_{\mathfrak{t}}x < r_2(\mathfrak{t}) = \mathrm{ord}_{\mathfrak{t}}\bar{x},$$
$$r_2(\mathfrak{t}) = \mathrm{ord}_{\mathfrak{t}}\bar{x} < r_1(\mathfrak{t}) = \mathrm{ord}_{\mathfrak{t}}x.$$

In the first case, $\mathrm{ord}_{\mathfrak{t}} 2\alpha y_1 \geq r(\mathfrak{t})$. In the second case,

$$\mathrm{ord}_{\mathfrak{t}} 2\alpha y_1 = \mathrm{ord}_{\mathfrak{t}}x = r_1,$$

and in the third case

$$\mathrm{ord}_{\mathfrak{t}} 2\alpha y_1 = \mathrm{ord}_{\mathfrak{t}}\bar{x} = r_2.$$

Next let

$$\mathscr{Y}_0 = \{\mathfrak{p} \in \mathscr{P}(GME_2) : \mathrm{ord}_{\mathfrak{p}}x = \mathrm{ord}_{\mathfrak{p}}\bar{x} < 0\}$$
$$\mathscr{Y}_1 = \{\mathfrak{p} \in \mathscr{P}(GME_2) : \mathrm{ord}_{\mathfrak{p}}x < \mathrm{ord}_{\mathfrak{p}}\bar{x} \leq 0\}$$
$$\mathscr{Y}_2 = \{\mathfrak{p} \in \mathscr{P}(GME_2) : \mathrm{ord}_{\mathfrak{p}}\bar{x} < \mathrm{ord}_{\mathfrak{p}}x \leq 0\}$$

Observe that since $\mathrm{ord}_{\mathfrak{p}}x = \mathrm{ord}_{\bar{\mathfrak{p}}}\bar{x}$, where $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are primes conjugate over E_2M, we have that $\mathscr{Y}_2$ consists of the conjugates over E_2 of primes in $\mathscr{Y}_1$, and $r_1(\mathfrak{p}) = r_2(\bar{\mathfrak{p}})$. Further $\mathscr{Y}_0$ is closed under conjugation. As above, let $\frac{\mathfrak{X}}{\mathfrak{Y}}$, $\frac{\overline{\mathfrak{X}}}{\overline{\mathfrak{Y}}}$, where $\mathfrak{X}, \mathfrak{Y}, \overline{\mathfrak{X}}, \overline{\mathfrak{Y}}$ are integral divisors and $(\mathfrak{X}, \mathfrak{Y}) = (\overline{\mathfrak{X}}, \overline{\mathfrak{Y}}) = 1$, be the GME_2-divisors of x and $\bar{x}$ respectively, and let $\frac{\mathfrak{B}}{\mathfrak{C}}$, where $\mathfrak{B}, \mathfrak{C}$ are integral relatively prime divisors, be the GME_2-divisor of $2\alpha y_1$. Then we can write

$$\mathfrak{Y} = \prod_{\mathfrak{p} \in \mathscr{Y}_0} \mathfrak{p}^{r(\mathfrak{p})} \prod_{\mathfrak{p} \in \mathscr{Y}_1 \cup \mathscr{Y}_2} \mathfrak{p}^{r_1(\mathfrak{p})},$$

and

$$\bar{\mathfrak{Y}} = \prod_{\bar{\mathfrak{p}} \in \mathscr{Y}_0} \bar{\mathfrak{p}}^{r(\bar{\mathfrak{p}})} \prod_{\bar{\mathfrak{p}} \in \mathscr{Y}_1 \cup \mathscr{Y}_2} \bar{\mathfrak{p}}^{r_1(\bar{\mathfrak{p}})} = \prod_{\mathfrak{p} \in \mathscr{Y}_0} \mathfrak{p}^{r(\mathfrak{p})} \prod_{\mathfrak{p} \in \mathscr{Y}_1 \cup \mathscr{Y}_2} \mathfrak{p}^{r_2(\mathfrak{p})}.$$

Consequently,

$$\mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{Y}) = \mathbf{N}_{E_2M/\mathbb{Q}}(\mathbf{N}_{GME_2/E_2M}\mathfrak{Y}) = \mathbf{N}_{E_2M/\mathbb{Q}}(\mathfrak{Y}\overline{\mathfrak{Y}}) = \mathbf{N}_{E_2M/\mathbb{Q}}\left(\prod_{\mathfrak{p}\in\mathscr{Y}_0}\mathfrak{p}^{2r(\mathfrak{p})}\prod_{\mathfrak{p}\in\mathscr{Y}_1\cup\mathscr{Y}_2}\mathfrak{p}^{r_1(\mathfrak{p})+r_2(\mathfrak{p})}\right).$$

Next we note that

$$\mathfrak{C} = \prod_{\mathfrak{p}\in\mathscr{Y}_0}\mathfrak{p}^{r_0(\mathfrak{p})}\prod_{\mathfrak{p}\in\mathscr{Y}_1}\mathfrak{p}^{r_1(\mathfrak{p})}\prod_{\mathfrak{p}\in\mathscr{Y}_2}\mathfrak{p}^{r_2(\mathfrak{p})},$$

where $r_0(\mathfrak{p}) \leq r(\mathfrak{p})$. Since the conjugate of $2\alpha y_1$ over ME_2 is $-2\alpha y_1$, we have that $\bar{\mathfrak{C}} = \mathfrak{C}$ and thus

$$\mathbf{N}_{GME_2/\mathbb{Q}}\mathfrak{C} = \mathbf{N}_{E_2M/\mathbb{Q}}(\mathbf{N}_{GME_2/E_2M}(\mathfrak{C})) = \mathbf{N}_{E_2M/\mathbb{Q}}(\mathfrak{C}\bar{\mathfrak{C}}) = \mathbf{N}_{E_2M/\mathbb{Q}}\left(\prod_{\mathfrak{p}\in\mathscr{Y}_0}\mathfrak{p}^{2r_0(\mathfrak{p})}\prod_{\mathfrak{p}\in\mathscr{Y}_1}\mathfrak{p}^{2r_1(\mathfrak{p})}\prod_{\mathfrak{p}\in\mathscr{Y}_2}\mathfrak{p}^{2r_2(\mathfrak{p})}\right),$$

Now it is clear that $\mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{C})\Big|\mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{Y})^2$.

Since on the one hand x does not have positive order at any prime of $\overline{\mathscr{Z}}_{GME_2}$, as in Lemma 6.5, we can conclude that $\mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{X})$ and $\mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{Y})$ are relatively prime as $\mathbb{Q}$-divisors. Thus, $\mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{Y})$ is the divisor of Y. On the other hand, if we let $\frac{B}{C} = \mathbf{N}_{GME_2/\mathbb{Q}}(2\alpha y_1)$, where $B, C \in \mathbb{Z}$ and are relatively prime in $\mathbb{Z}$, then certainly $C\Big|\mathbf{N}_{GME_2/\mathbb{Q}}(\mathfrak{C})$. Thus, $\frac{Y^2}{Z}\mathbf{N}_{GME_2/\mathbb{Q}}(2\alpha y_1)$ will have no rational primes lying below the primes of $\mathscr{Z}_{GME_2}$ in the denominator. Further, by assumption, as in Lemma 6.5 we have that for all primes $\mathfrak{t}$ such that $\mathrm{ord}_{\mathfrak{t}}\mathfrak{Z} > 0$ it is the case that $\mathrm{ord}_{\mathfrak{t}}x \geq \mathrm{ord}_{\mathfrak{t}}\mathfrak{Z}$ and $\mathrm{ord}_{\mathfrak{t}}\bar{x} \geq \mathrm{ord}_{\mathfrak{t}}\mathfrak{Z}$. Therefore, $\mathrm{ord}_{\mathfrak{t}}(x-\bar{x}) \geq \mathrm{ord}_{\mathfrak{t}}\mathfrak{Z}$ and consequently,

$$\mathrm{ord}_{\mathfrak{t}}2\alpha y_1 = \mathrm{ord}_{\mathfrak{t}}(x-\bar{x}) \geq \mathrm{ord}_{\mathfrak{t}}\mathfrak{Z}.$$

□

The next lemma follows from the fact that $Q(X) \in \mathbb{Z}[X]$ has a positive leading coefficient.

Lemma 6.7. *For any positive integer k there exists a number $A(k) > 1$ such that for any real $x > A(k)$, we have that $Q(x) > k$.*

Notation 6.8. For future use we introduce the following notation.

- Let $B = A(2) + 1$.

The following lemma will allow us to establish some bounds on coordinates in a degree 2 extension of a totally real field.

Lemma 6.9. *Let $y \in E_2GM$ and let $x = y_0 + y_1\alpha, y_0, y_1 \in E_2M$. Let $z \in E_2GM$ and suppose that for every $\sigma_1, \ldots, \sigma_{pr_{GM}} : E_2GM \longrightarrow \tilde{\mathbb{Q}} \cap \mathbb{R}$, we have that*

$$1 \leq |\sigma_i(x)| < |\sigma_i(z)|, \tag{6.3}$$

while for all $\tau_1, \ldots, \tau_{ps_{GM}} : E_2GM \longrightarrow \tilde{\mathbb{Q}}$ with $\tau_i(E_2GM) \not\subseteq \mathbb{R}$, we have that

$$|\tau_i(z)| \geq 1 \tag{6.4}$$

Then $|\mathbf{N}_{GME_2/\mathbb{Q}}(y_1)| \leq |\mathbf{N}_{GME_2/\mathbb{Q}}(z)\mathbf{N}_{GME_2/\mathbb{Q}}(x)|$.

Proof. First of all observe that for all non-real embeddings $\tau_i : E_2GM \to \tilde{\mathbb{Q}}$, we have that $\overline{\tau_i(x)} = \tau_i(y_0) - \tau_i(\alpha)\tau_i(y_1)$ and therefore,

$$|\tau_i(y_1)| = \left|\frac{\tau_i(x) - \overline{\tau_i(x)}}{2\tau_i(\alpha)}\right| \leq \left|\frac{\tau_i(x)}{\tau_i(\alpha)}\right| < |\tau_i(x)|, \tag{6.5}$$

since by assumption $|\tau_i(\alpha)| > 1$. On the other hand, for any real embedding $\sigma_i : E_2GM \to \tilde{\mathbb{Q}}$, we have that $\sigma_i(x) = \sigma_i(y_0) + \sigma_i(\alpha)\sigma_i(y_1)$, while for some $i' \in \{1, \ldots, pr_{GM}\}$ we also have that $\sigma_{i'}(x) = \sigma_i(y_0) - \sigma_i(\alpha)\sigma_i(y_1)$. Thus,

$$|\sigma_i(y_1)| = \left|\frac{\sigma_i(x) - \sigma_{i'}(x)}{2\sigma_i(\alpha)}\right| \leq \left|\frac{2\sigma_i(z)}{2\sigma_i(\alpha)}\right| < |\sigma_i(z)|, \tag{6.6}$$

Putting together (6.5) and (6.6) we obtain,

$$|\mathbf{N}_{E_2GM/\mathbb{Q}}(y_1)| \leq \prod_{\tau_i} |\tau_i(x)| \prod_{\sigma_j} |\sigma_j(z)| \leq |\mathbf{N}_{GME_2/\mathbb{Q}}(xz)|, \tag{6.7}$$

where the last inequality follows from (6.3) and (6.4). □

Lemma 6.10. *Let $x \in GME_2$. Let $l > 2$ be an integer such that $l > \max(\{|\beta_j|, j = 1, \ldots, p_2\})$. Let $x_k = Q(x - 8(k+1)l)$. Then for some value of $k \in \{0, \ldots, 2p_2n\}$ we have that for any embedding $\phi : GME_2 \to \tilde{\mathbb{Q}}$, it is the case that $|\phi(x_k)| > 2$. (Here we remind the reader that from Notation and Assumptions 5.1 we have that $n = [M : \mathbb{Q}]$, $[E_2M : M] = p_2$, and $[E_2GM : E_2M] = 2$.)*

Proof. In GME_2 we can factor

$$Q(x - 8(k+1)l) = \prod_{j=1}^{p_2} (N_{\mathscr{E}}x - 8(k+1)l - \beta_j).$$

Let $B_k \subset \mathbb{C}$ be the closed ball of radius $2l$ centered at $8(k+1)l$ (i.e. $B_k = \{z \in \mathbb{C} : |z - (8(k+1)l)| \leq 2l\}$). We claim that for all j, k it is the case that $\beta_j + 8(k+1)l \in B_k$. Further, the distance between any point of B_k and any point of $B_{k'}$ for $k \neq k'$ is at least $4l \geq 4$ and so $B_k \cap B_{k'} = \emptyset$ for $k \neq k'$.

Let $\phi_1, \ldots, \phi_{2p_2n}$ be all the embeddings of E_2GM over $\mathbb{Q}$. Then each $\phi_i(N_{\mathscr{E}}x)$ can be located in at most one B_k. Further, if $\phi_i(N_{\mathscr{E}}x) \notin B_k$ then for any j we have that $|\phi_i(N_{\mathscr{E}}x) - \beta_j - 8(k+1)l| > l > 2$. Since there is at least one B_k without any $\phi_i(N_{\mathscr{E}}x)$'s, for some $k = \{0, \ldots, 2p_2n\}$, for all i, j, we have that

$$|\phi_i(N_{\mathscr{E}}x) - 8l(k+1) - \beta_j| > 2$$

implying that for all i we have that

$$\phi_i(Q(x - 8(k+1)l)) = \phi_i(P(N_{\mathscr{E}}x - 8(k+1)l)) = \prod_{j=1}^{p} (\phi_i(N_{\mathscr{E}}x) - 8(k+1)l - \beta_j) \geq 2.$$

□

7. **Diophantine Definability for Extensions of Degree 2.**

In this section we consider two versions of Diophantine definability for extensions of degree 2 of totally real fields. In the first version we will restrict ourselves to the ring $O_{GME_2, \mathscr{U}_{GME_2}}$, but the definition will not use the degree of GM over $\mathbb{Q}$. In the second version we will use explicitly the degree of GM over $\mathbb{Q}$ but allow any prime of $\mathscr{Z}_{E_2GM}$ in the denominator.

Notation 7.1. We add the following to our notation and assumption list.

- Let l be as in Lemma 6.10, i.e. let $l \in \mathbb{Z}_{>0}$ be an upper bound for the absolute values of all the roots of $P(X)$.

We start with a technical lemma.

Lemma 7.2. *Let $\varepsilon \in O_{HGME_2}$ be a solution to (5.1). Then for any positive integer k and any $\lambda > 0$ there exists a positive integer r such that for all $\tau : GME_2H \to \tilde{\mathbb{Q}}$ with $\tau(E_2HM) \not\subset \mathbb{R}$ we have that*

$$\left| \frac{\tau(\varepsilon^{rk} - 1)}{\tau(\varepsilon^r - 1)} - k \right| < \lambda.$$

Proof. We start with an elementary observation:

$$T^k - 1 = (T - 1 + 1)^k - 1 = \sum_{i=1}^{k} \frac{k!}{i!(k-i)!} (T-1)^i = \sum_{i=1}^{k} \binom{k}{i} (T-1)^i,$$

and so

$$\frac{T^k - 1}{T - 1} = \sum_{i=1}^{k} \frac{k!}{i!(k-i)!} (T-1)^{i-1} = \sum_{i=1}^{k} \binom{k}{i} (T-1)^{i-1}$$

Assume that k and $0 < \lambda < 1$ are fixed and suppose $z \in \mathbb{C}$ is such that $|z-1| < 2^{-k}\lambda$. Then

$$\left|\frac{z^k-1}{z-1} - k\right| = \left|\sum_{i=2}^{k} \left(\begin{array}{c} k \\ i \end{array} \right) (z-1)^{i-1}\right| \leq 2^{-k}\nu \sum_{i=0}^{k} \left(\begin{array}{c} k \\ i \end{array} \right) = \lambda.$$

Now let $\varepsilon \in O_{GME_2H}$ be a solution to (5.1). Let m be defined as in Corollary 5.4 and deduce that $\varepsilon^m \in E_2MH$ with $|\tau(\varepsilon^m)| = 1$ for all τ, non-real embeddings of E_2MH into $\tilde{\mathbb{Q}}$. Thus, given $\nu > 0$ and k the problem reduces to showing that for some power $r \cong 0 \mod m$ of ε we will have $|\tau(\varepsilon)^r - 1| < 2^{-k}\nu$ for all non-real embeddings of E_2HM into $\tilde{\mathbb{Q}}$. The proof of this fact is completely analogous of the proof of Lemma 12 of [22]. □

Lemma 7.3. *Let*

$$x_0, x_1 \in O_{GM,\mathscr{U}_{GM}},$$
$$a_1, a_2, b_1, b_2, c, d, u, v \in O_{GM,\mathscr{U}_{GM}}[\mu] \subset O_{E_2GM,\mathscr{U}_{GME_2}},$$
$$\varepsilon_i, \gamma_i \in O_{GM,\mathscr{U}_{GM}}[\mu,\delta] \subset O_{E_2GMH,\mathscr{U}_{E_2GMH}}, i = 1,\ldots,4.$$

Assume also that the following conditions and equations are satisfied.

$$\forall \mathfrak{p} \in \overline{\mathscr{E}}_{GM},\ ord_{\mathfrak{p}} x_0 \geq 0 \tag{7.1}$$

$$x_1 = Q(x_0), \tag{7.2}$$

$$\left\{ \begin{array}{l} \mathbf{N}_{HGME_2/EGM}(\varepsilon_i) = 1, i = 1,\ldots,4, \\ \mathbf{N}_{GMHE_2/HGM}(\varepsilon_i) = 1, i = 1,\ldots,4, \end{array} \right. \tag{7.3}$$

$$\gamma_i = \varepsilon_i^m, \gamma_i \neq 1, i = 1,\ldots,4, \tag{7.4}$$

$$\frac{\gamma_{2j}-1}{\gamma_{2j-1}-1} = a_j - \delta b_j, j = 1,2 \tag{7.5}$$

$$\gamma_3 = c + \delta d, \tag{7.6}$$

$$1 \leq |\sigma(x_1)| \leq Q(B + \sigma(a_1^2 - db_1^2)^2), \tag{7.7}$$

where σ ranges over all real embedding of E_2GM into $\tilde{\mathbb{Q}}$,

$$x_1 - (a_2 - \delta b_2) = (c - 1 + \delta d)(u + v\delta), \tag{7.8}$$

$$Px_1Q(B + (a_1^2 - db_1^2)^2) \big| (c - 1 + \delta d), \tag{7.9}$$

where P is a rational prime without any factors in $\mathscr{U}_{GMHE_2}$. (For example, P can be any prime splitting completely in the extension $\mathbb{Q}(\mu)/\mathbb{Q}$.) Then $x_1 \in M$.

Conversely, if $x_0 \in \mathbb{N}$, the conditions and equations above can be satisfied in variables ranging over the prescribed sets.

Proof. From (7.3), (7.4) and Corollary 5.4 we conclude that for all $i = 1,\ldots,4$, we have that $\gamma_i \in O_{HE_2M}$. Therefore, $c, d \in O_{E_2GM,\mathscr{U}_{E_2GM}}$. Since δ generates HE_2M over E_2M and E_2GMH over E_2GM, we conclude that $c, d \in O_{E_2M,\mathscr{U}_{E_2M}}$. A similar argument tells us that $a_1, b_1, a_2, b_2 \in O_{E_2M,\mathscr{U}_{E_2M}}$.

Next from (7.2) and Lemma 6.2 we conclude that for all $\mathfrak{p} \in \overline{\mathscr{U}}_{GME_2}$ we have that $\mathrm{ord}_{\mathfrak{p}} x_1 \leq 0$ and

$$\mathrm{ord}_{\mathfrak{p}} Q(B + (a_1^2 - db_1^2)^2) \leq 0.$$

From definition of B (see Notation 6.8) and the fact that $a_1, b_1 \in E_2M$ - a totally real field, we have that

$$1 \leq Q(B + \tau(a_1^2 - db_1^2)^2), \tag{7.10}$$

where τ ranges over all non-real embeddings of GME_2 into $\tilde{\mathbb{Q}}$. Combining the bound equations (7.7) and (7.10), and writing $x_1 = y_0 + y_1\alpha$, where $y_0, y_1 \in O_{M,\mathscr{U}_M}$, we conclude by Lemma 6.9

$$|\mathbf{N}_{E_2GM/\mathbb{Q}}(2\alpha y_1)| \leq |\mathbf{N}_{E_2GM/\mathbb{Q}}(x_1)\mathbf{N}_{E_2GM/\mathbb{Q}}(Q(B + (a_1^2 - db_1^2)^2))|. \tag{7.11}$$

Next consider the divisor $\mathfrak{D}$ of $c - 1 + \delta d$. We can write as $\mathfrak{D} = \mathfrak{D}_1\mathfrak{D}_2$, where

$$\mathfrak{D}_1 = \prod_{\mathfrak{q} \notin \mathscr{U}_{GME_2H}} \mathfrak{q}^{\mathrm{ord}_{\mathfrak{q}}(c-1+\delta d)}$$

is an integral divisor, and $\mathfrak{D}_2$ is comprised of primes of $\mathscr{U}_{GME_2H}$ only. Observe that from (7.8), we have that

$$x_1 - (a_2 - b_2\delta) \cong 0 \mod \mathfrak{D}_1 \text{ in } O_{GMHE_2,\mathscr{U}_{GME_2H}}$$

Let

$$D_1 = |\mathbf{N}_{E_2GMH/\mathbb{Q}}(\mathfrak{D}_1)| \in \mathbb{Z}_{>0},$$

let

$$|\mathbf{N}_{E_2GMH/\mathbb{Q}}(x_1)| = \frac{X}{Y},$$

and let

$$|\mathbf{N}_{E_2GMH/\mathbb{Q}}(B + Q(a_1^2 - db_1^2))| = \frac{U}{V},$$

where $X, Y, U, V \in \mathbb{Z}_{>0}, (X, Y) = 1, (U, V) = 1$, and X, U are not divisible by any rational primes with factors in $\mathscr{U}_{GME_2H}$. Then from (7.9) we have that

$$XU < D_1. \tag{7.12}$$

By Lemma 6.5, on the one hand we have that

$$\frac{Y\mathbf{N}_{E_2GMH/\mathbb{Q}}(2\alpha y_1)}{D_1} \in \mathbb{Z},$$

and therefore

$$|Y\mathbf{N}_{E_2GMH/\mathbb{Q}}(2\alpha y_1)| \geq D_1 \text{ or } y_1 = 0.$$

On the other hand, combining (7.11) and (7.12), we have that $|Y\mathbf{N}_{E_2GMH/\mathbb{Q}}(2\alpha y_1)| \leq XU < D_1$. Thus y_1 is 0 and $x_1 \in M$.

We will now show that assuming that $x_0 > 0$ is a natural number, we can satisfy all the equations and conditions (7.2)–(7.9). Observe that by (7.2), we have that x_1 is also a natural number. Let $\nu \in U_{E_2HM} \cap O_M[\delta, \mu]$ be a solution to (5.1) such that it is not a root of unity. Such a solution exists by Lemma 5.2, Corollary 5.4 and by Section 2.1.1 of [26]. Let $\{\phi_1, \ldots, \phi_{s_{E_2HM}}\}$ be a set containing a representative from every complex-conjugate pair of non-real conjugates of ν. By Lemma 7.2, we can find a positive integer $r \cong 0 \mod m$ such that for all $i = 1, \ldots, s_{E_2HM}$ we have that

$$\left| \frac{\phi_i^{rA} - 1}{\phi_i^r - 1} - A \right| < \frac{1}{2},$$

where $A = A(x_1) + 1$ (see Lemma 6.7), and thus,

$$\left| \frac{\phi_i^{rA} - 1}{\phi_i^r - 1} \right| > A - \frac{1}{2} > A(x_1).$$

So we set $\varepsilon_1 = \nu^{r/m}, \gamma_1 = \varepsilon^r, \varepsilon_2 = \varepsilon^{rA/m}, \gamma_2 = \varepsilon^{rA}$. Then for $i = 1, 2$ the system (7.3) is satisfied. We also satisfy (7.4) for these values of i. Next we define a_1 and b_1 so that (7.5) is satisfied for $j = 1$. Next let σ be an embedding of M into $\tilde{\mathbb{Q}}$ extending to a real embedding of GM and therefore to a real embedding of GME_2. Then by assumption on H, we have that σ extends to a non-real embedding $\hat{\sigma}$ on E_2MH. Thus, without loss of generality, for some $i = 1, \ldots, s_{E_2HM}$ we have that

$$\hat{\sigma}(a_1 - \delta b_1) = \hat{\sigma}\left(\frac{\varepsilon^{rA} - 1}{\varepsilon^r - 1}\right) = \frac{\phi_i^{rA} - 1}{\phi_i^r - 1},$$

and therefore

$$\sigma(a_1^2 - db_1^2) = \left| \frac{\phi_i^{rA} - 1}{\phi_i^r - 1} \right|^2 > A(x_1)^2 > A(x_1),$$

leading to

$$Q(B+\sigma(a_1^2-db_1^2)^2)>x_1=\sigma(x_1)>1.$$

Thus we can satisfy (7.7).

Let ε_3 to be a solution to (7.3) in $O_{GM}[\delta,\mu]$ such that $\gamma_3=\varepsilon_3^m\in U_{E_2MH}\cap O_M[\delta,\mu]$, (7.4), (7.6) for $i=3$, and (7.9) are satisfied. Again this can be done by Lemma 5.2, Corollary 5.4 and by Section 2.1.1 of [26]. Finally, set $\varepsilon_4=\varepsilon_3^{x_1},\gamma_4=\gamma_3^{x_1}$. In this case we can satisfy (7.3), (7.6) for $i=4$.

We now observe that

$$a_2-\delta b_2=\frac{\gamma_4-1}{\gamma_3-1}=x_1+(\gamma_3-1)(u+\delta v)=x_1+(c-1-\delta d)(u+v\delta),$$

where $u,v\in O_{GM,\mathscr{U}_{GM}}[\mu]$. Thus (7.8) will also be satisfied. □

Next we prove a slightly different version of the result above. We will explicitly use the degree of M over $\mathbb{Q}$.

Lemma 7.4. *Let $x,x_0,\dots,x_{2p_2n}\in O_{GM,\mathscr{Z}_{GM}},a_0,b_0,\dots,a_{2p_2n},b_{2p_2n},v,u\in O_{GM,\mathscr{Z}_{GM}}[\mu]\subset O_{GME_2H,\mathscr{Z}_{GME_2H}}$, $\varepsilon_i,\gamma_i\in O_{GM,\mathscr{Z}_{GM}}[\mu,\delta]\subset O_{GME_2H,\mathscr{Z}_{GME_2H}},i=0,\dots,2p_2n$. Assume also that the following equations hold.*

$$\forall\mathfrak{p}\in\overline{\mathscr{E}}_{GM},\ ord_{\mathfrak{p}}x_0\geq 0 \tag{7.13}$$

$$x_k=Q(x+8l(k+1)),k=0,\dots,2p_2n \tag{7.14}$$

$$\begin{cases}\mathbf{N}_{HGME_2/E_2GM}(\varepsilon_i)=1,i=0,\dots,2p_2n,\\ \mathbf{N}_{GMHE_2/HGM}(\varepsilon_i)=1,i=0,\dots,2p_2n,\end{cases} \tag{7.15}$$

$$\gamma_i=\varepsilon_i^m,\gamma_i\neq 1,i=0,\dots,2p_2n, \tag{7.16}$$

$$\frac{\gamma_{j+1}-1}{\gamma_0-1}=a_j-\delta b_j,j=0,\dots,2p_2n \tag{7.17}$$

$$\gamma_0=c+\delta d, \tag{7.18}$$

$$x_j-(a_j-\delta b_j)=(c+\delta d)(u+v\delta),j=0,\dots,2p_2n \tag{7.19}$$

$$\left(\prod_{j=0}^{2p_2n}x_j^2\right)\Big|(c_0-1+\delta d_0)\ in\ O_{E_2GMH,\mathscr{Z}_{E_2GMH}}. \tag{7.20}$$

Then for some $j\in\{0,\dots,2p_2n\}$ we have $x_j\in M$. Conversely, if $x_0\in\mathbb{Z}_{>0}$, then equations (7.14) – (7.20) can be satisfied with all the variables in the prescribed sets.

Proof. We start as in Lemma 7.3 with concluding that $\gamma_j\in E_2HM$ for all $j=0,\dots,2p_2n$, and therefore $a_j,b_j\in O_{E_2M,\mathscr{W}_{E_2M}}$. Also as in Lemma 7.3, we note that $\mathrm{ord}_{\mathfrak{p}}x_k\leq 0$ for all $\mathfrak{p}\in\mathscr{Z}_{GME_2H}$. By Lemma 6.10, for some j we have that that all the $\mathbb{Q}$-conjugates of x_j have absolute value greater than 2. Further, if $x_j=y_{0,j}+y_{1,j}\alpha$,where $y_{0,j},y_{1,j}\in M$, $\bar{x}_j$ is the conjugate of x_j over M, and $\rho:GM\to\tilde{\mathbb{Q}}$ is an embedding of GM into its algebraic closure, then

$$|2\rho(\alpha y_{1,j})|=|\rho(x_j)-\rho(\bar{x}_j)|\leq 2\max\{|\rho(x_j)|,|\rho(\bar{x}_j)|\}<|\rho(x_j)\rho(\bar{x}_j)|.$$

Thus,

$$|\mathbf{N}_{GMHE_2/\mathbb{Q}}(2\alpha y_{1,j})|<|\mathbf{N}_{GMHE_2/\mathbb{Q}}(x_j\bar{x}_j)|=|\mathbf{N}_{GMHE_2/\mathbb{Q}}(x_j)\mathbf{N}_{GMHE_2/\mathbb{Q}}(\bar{x}_j)|=\mathbf{N}_{GMHE_2/\mathbb{Q}}(x_j^2). \tag{7.21}$$

Next consider the divisor $\mathfrak{D}$ of $c-1+\delta d$. We can write as $\mathfrak{D}_1\mathfrak{D}_2$, where

$$\mathfrak{D}_1 = \prod_{\mathfrak{q}\not\in\mathscr{Z}_{GME_2H}} \mathfrak{q}^{\mathrm{ord}_{\mathfrak{q}}(c-1+\delta d)},$$

is an integral divisor and $\mathfrak{D}_2$ is divisible by primes of $\mathscr{Z}_{GME_2H}$ only. Observe that from (7.19), we have that

$$x_j - (a_j - b_j\delta) \cong 0 \mod \mathfrak{D}_1$$

in $O_{E_2GMH,\mathscr{W}_{E_2GMH}}$. Let

$$D_1 = |\mathbf{N}_{E_2GMH/\mathbb{Q}}(\mathfrak{D}_1)|,$$

and let

$$|\mathbf{N}_{E_2GMH/\mathbb{Q}}(x_j)| = \frac{X_j}{Y_j}.$$

Then by Lemma 6.6 we conclude that

$$\frac{Y_j^2\mathbf{N}_{GME_2H/\mathbb{Q}}(2\alpha y_{1,j})}{D} \in \mathbb{Z} \Rightarrow |Y_j^2\mathbf{N}_{GME_2H/\mathbb{Q}}(2\alpha y_{1,j})| \geq D_1,$$

unless $y_{1,j} = 0$. At the same time, we also have from (7.20) that $X_j^2 \leq D_1$, and further from (7.21) we deduce that

$$|Y_j^2\mathbf{N}_{GME_2H/\mathbb{Q}}(2\alpha y_{1,j})| < Y_j^2\mathbf{N}_{GMHE_2/\mathbb{Q}}(x_j^2) = X_j^2 \leq D_1.$$

Hence we must conclude that $y_{1,j} = 0$.

The argument that the equations above can be satisfied if x is a positive integer is analogous to the argument used in Lemma 7.3. □

8. **Diophantine Definability and Decidability in Big Subrings of Extensions of Degree 2 of Totally Real Number Fields.**

In this section we will use the technical results from Sections 5, 6, and 7 to show that in *any* extension of a degree 2 of a totally real number field, the elements of $\mathbb{Q}$ contained in some big rings have a Diophantine definition over these rings. Given this definability result, by now well-explored technique will immediately produce a Diophantine definition of $\mathbb{Z}$ in smaller (but still big) subrings, as well as a counter examples for the archimedean and non-archimedian versions of a Mazur's conjecture over these rings.

We start with observing that we have done most of the work in proving the following definability result.

Proposition 8.1. *$O_{GM,\mathscr{Z}_{GM}} \cap M$ has a Diophantine definition over $O_{GM,\mathscr{Z}_{GM}}$.*

Proof. Lemma 7.4 will serve as the basis of our proof. First, we define recursively several constants. Let N_1 be a positive integer such that for a any $k, k' \in \{0,\ldots,2p_2n\}$, we have that polynomials $Q(X+8l(k+1))$ and $Q(X+N_1+8l(k'+1))$ are linearly independent over $\mathbb{C}$. Such a N_1 exists by Lemma 12.1. Assume, $N_1,\ldots,N_s, s < p_2$ have been defined recursively, and define N_{s+1} to be a natural number such that for any $k_0,\ldots,k_s,k_{s+1} \in \{0,\ldots,2p_2n\}$ we have that the set of polynomials

$$\{Q(X+8l(k_0+1)), Q(X+N_1+8l(k_1+1)),\ldots,Q(X+N_s+8l(k_s+1)), Q(X+N_{s+1}+8l(k_{s+1}+1))\}$$

is linearly independent over $\mathbb{C}$. As above, N_{s+1} exists by Lemma 12.1.

Let $N_0 = 0$ and suppose now that Equations (7.14)–(7.20) are satisfied for $x = y+N_0, y+N_1,\ldots,y+N_{p_2}$, where $y \in O_{GM,\mathscr{Z}_{GM}}$. Then by Lemma 7.4, for some $k_0,\ldots,k_{p_2} \in \{0,\ldots,2p_2n\}$ we have that

(1) $Q(y+N_s+8l(k_s+1)) \in O_{M,\mathscr{V}_M}$ for $s = 0,\ldots,p_2$,
and
(2) the set of polynomials $\{Q(X+N_s+8l(k_s+1)), s = 0,\ldots,p_2\}$ is linearly independent of $\mathbb{C}$.

Therefore, by Lemma 5.1 of [25] we have that $y \in O_{M,\mathscr{Z}_M}$. We also know by Lemma 7.14 that if y is a positive integer then all the equations can be satisfied with variables taking values in the prescribed sets. To get all the other elements of $O_{M,\mathscr{Z}_M}$ we can use any integral basis of M over $\mathbb{Q}$. Thus the only remaining task is making sure that all the Equations (7.14)–(7.20) can be rewritten in polynomial form with variables ranging over $O_{GM,\mathscr{Z}_{GM}}$. We can rewrite all the equations with coefficients and variable in $O_{GM,\mathscr{Z}_{GM}}$ instead of $O_{GME,\mathscr{Z}_{GME_2}}$ and $O_{GMEH,\mathscr{Z}_{GME_2H}}$ by Proposition 2.7 and Proposition 2.8. □

We can summarize the discussion of the degree 2 extensions of totally real number fields in the following theorem.

Theorem 8.2. *Let K be a totally real number field. Let G be any extension of K of degree 2. Let T be any totally real cyclic extension of $\mathbb{Q}$ of odd prime degree $p > 0$ such that p does not divide the degree of the Galois closure of K over $\mathbb{Q}$. Let $E = KT$. Let $\mathscr{X}_G$ be a set of primes of G such that all but finitely primes of $\mathscr{X}_G$ are not splitting in the extension GE/G. Then $O_{G,\mathscr{X}_G} \cap K$ has a Diophantine definition over $O_{G,\mathscr{X}_G}$.*

Proof. Let K_G be the Galois closure of K over $\mathbb{Q}$. Given our assumption on p, we have that

$$[EK_G : K_G] = [EG : G] = [E : K] = [T : \mathbb{Q}] = p$$

and a rational prime $\mathfrak{P}$ does not split in the extension $T/\mathbb{Q}$ if and only if all of its factors in K and G do not split in the extensions E/K and EG/G respectively by Lemmas 12.4 and 12.6. Further any generator μ of T over $\mathbb{Q}$ will also generate E over K. Thus if $P(X)$ is the monic irreducible polynomial of μ over K or over GK, it will have rational integer coefficients. Since $p \geq 3$, by Dirichlet Unit Theorem we have that T has units which are not roots of unity. We can set μ to be such a unit and satisfy Notation and Assumptions 6.1.

Given that we can define integrality at finitely many primes over number fields (see Proposition 2.2), we can restrict all the variables to the values in $O_{G,\mathscr{X}_G}$ integral at all the primes splitting in the extension EG/G or dividing the discriminant of $P(X)$ (this set of "inconvenient" primes was denoted by $\mathscr{E}_G$). Note that we can reconstruct all the values in the ring $O_{G,\mathscr{X}_G}$ by taking the ratios of the variables whose values are restricted. This is so because we have an existential definition of all the non-zero values from Proposition 2.3. Then by Proposition 8.1 we conclude that $O_{G,\mathscr{X}_G} \cap K$ has a Diophantine definition over $O_{G,\mathscr{X}_G}$. □

We should note next that the theorem above is a (stronger) analog of Theorem 3.6 and Corollary 3.7 of [28] where a similar result was proved for totally complex extensions of degree 2 of totally real fields. Now using almost exactly the same method as in [28] we can derive analogs of Theorems 3.8, 3.10, 3.11, 3.12, and 3.14 of [28]. Further using the natural version of the Tchebotarev density theorem (see [19]), we can replace Dirichlet density by natural density in the statements of all the propositions. We list the statements of these theorems below.

Theorem 8.3. *Let $K, G, E, \mathscr{X}_G$ be as in Theorem 8.2. Then there exists a set of G-primes $\mathscr{N}_G$ such that $\mathscr{X}_G \subseteq \mathscr{N}_G$, $\mathscr{N}_G \setminus \mathscr{X}_G$ is a finite set, and $O_{G,\mathscr{N}_G} \cap \mathbb{Q}$ has a Diophantine definition over $O_{G,\mathscr{N}_G}$.*

Theorem 8.4. *Let G be any extension of degree 2 of a totally real field. Let $\mathscr{Y}_G$ be any set of primes of G. Then for any $\varepsilon > 0$ there exists a set $\mathscr{D}_G$ such that $\mathscr{Y}_G \setminus \mathscr{D}_G$ is contained in a set of natural density less than ε, $\mathscr{D}_G \setminus \mathscr{Y}_G$ is finite, and $O_{G,\mathscr{D}_G} \cap \mathbb{Q}$ has a Diophantine definition over $O_{G,\mathscr{D}_G}$.*

Theorem 8.5. *Let $\mathscr{Y}_\mathbb{Q}$ be any set of rational primes. Then for any $\varepsilon > 0$ and any degree 2 extension G of a totally real number field, there exists a set of rational primes $\mathscr{D}_\mathbb{Q}$ such that $\mathscr{D}_\mathbb{Q} \setminus \mathscr{Y}_\mathbb{Q}$ is finite, $\mathscr{Y}_\mathbb{Q} \setminus \mathscr{D}_\mathbb{Q}$ is contained in a set of primes of natural density less than ε, and $O_{\mathbb{Q},\mathscr{D}_\mathbb{Q}}$ has a Diophantine definition in its integral closure in G.*

Theorem 8.6. *Let G be any extension of degree 2 of a totally real number field. Let χ_G be the density of the set of rational primes splitting completely in G. Then for any $\varepsilon > 0$ there exists a recursive set $\mathscr{Y}_G$ of primes of G whose natural density is bigger than $1 - \chi_G - \varepsilon$ and such that $\mathbb{Z}$ has a Diophantine definition over $O_{G,\mathscr{Y}_G}$. (Thus, Hilbert's Tenth Problem is undecidable in $O_{G,\mathscr{Y}_G}$.)*

Corollary 8.7. *Let G be any extension of degree 2 of a totally real number field. Then for any $\varepsilon > 0$ there exists a recursive set $\mathscr{Y}_G$ of primes of G whose natural density is bigger than $1 - 1/[G : \mathbb{Q}] - \varepsilon$ and such that $\mathbb{Z}$ has a Diophantine definition over $O_{G,\mathscr{Y}_G}$.*

Theorem 8.8. *Let G be any extension of degree 2 of a totally real number field and let $\varepsilon > 0$ be given. Let $\mathscr{Y}_\mathbb{Q}$ be the set of all rational primes splitting in G. (If the extension is Galois but not cyclic, $\mathscr{Y}_\mathbb{Q}$ contains all the primes.) Then there exists a set of G-primes $\mathscr{D}_G$ such that the set of rational primes $\mathscr{D}_\mathbb{Q}$ below $\mathscr{D}_G$ differs from $\mathscr{Y}_\mathbb{Q}$ by a set contained in a set of natural density less than ε and such that $\mathbb{Z}$ has a Diophantine definition over $O_{G,\mathscr{D}_G}$.*

As we discussed in the introduction, given Theorem 8.3, we can also reproduce results concerning existential definability of discrete sets in the archimedean and non-archimedean topologies and a ring version of Mazur's conjecture on topology of rational points. The proof of these results depends on the analogs of Theorem 8.3 only and therefore can be lifted almost verbatim from the proofs of Theorem 3.6 of [29] and Theorem 1.8 of [18]. We state these two results below with Dirichlet density again replaced by natural density.

Theorem 8.9. *Let G be an extension of degree 2 of a totally real number field. Then for any $\varepsilon > 0$, there exists a recursive set of G-primes $\mathscr{Y}_G$ such that the natural density of $\mathscr{Y}_G$ is greater $1-\varepsilon$ and there exists an affine algebraic set V defined over G such that its intersection with $O_{G,\mathscr{Y}_G}$ is infinite and discrete in the usual archimedean topology, and therefore $\overline{V(O_{G,\mathscr{Y}_G})}$, the topological closure of the set of points of V which happen to be in $O_{G,\mathscr{Y}_G}$ in $\mathbb{C}$ if G is not real, and in $\mathbb{R}$, if G is real, has infinitely many connected components.*

Theorem 8.10. *Let G be a degree-2 extension of a totally real number field. Let $\mathfrak{p}$ be any prime of K and let $p_{\mathbb{Q}}$ be the rational prime below it. Then for any $\varepsilon > 0$ there exists a recursive set of G-primes $\mathscr{Y}_G \ni \mathfrak{p}$ of natural density $> 1-\varepsilon$ such that there exists an infinite Diophantine subset of $O_{G,\mathscr{Y}_G}$ that is discrete and closed when viewed as a subset of the completion $G_{\mathfrak{p}}$. In fact, such a subset can be found inside $\mathbb{Z}[1/p_{\mathbb{Q}}]$.*

9. Diophantine Decidability and Definability over Totally Real Infinite Extensions of $\mathbb{Q}$: an Update.

In this section using the updated version of the norm equations, we update some definability and decidability results for totally real infinite extensions of $\mathbb{Q}$. The main difference from our earlier results is in the fact that we will be able to include factors of any finite set of K primes in the allowed denominators for the rings under consideration, assuming these primes do not split in the extension K_∞/K.

Notation and Assumptions 9.1. In this section we will use the following notation and assumptions together with Notation and Assumptions 4.1, 5.1, 6.1, 6.3, and 6.8 which are now assumed to hold for any field M such that M is contained in a field K_∞ described below and $K \subset M$.

- Let K_∞ be a totally real normal algebraic extension of $\mathbb{Q}$ with $K \subset K_\infty$.
- Assume that only finitely many rational primes are ramified in K_∞.
- There are only finitely many primes p dividing $[M:K]$ for any number field M such that $K \subset M \subset K_\infty$.
- Let A be a positive constant.
- Assume that the extension K_∞/K satisfies the following conditions. For any number field M with $K \subset M \subset K_\infty$ besides assumptions described above, we also have that
  - There exists a subfield $\bar{M} \subset M$ such that $K \subset \bar{M}$ and $[M:\bar{M}] \leq A$.
  - There exists a basis $\Omega = \{\omega_1 = 1, \omega_2, \ldots, \omega_{n_M}\} \subset O_M$ of M over $\bar{M}$ such that for all embeddings σ of K_∞ into its algebraic closure, $|\sigma(\omega_j)| < A$.
- Let $D \in \mathbb{Z}_{>0}$ satisfy the following conditions.
  - For all $\mathfrak{p} \in \mathscr{W}_K$ we have that $\mathrm{ord}_{\mathfrak{p}} D = 0$.
  - D is greater than any conjugate of the discriminant of $\mathtt{D}_{M/\bar{M}}(\Omega)$ of Ω over $\mathbb{Q}$ for any Ω, M and $\bar{M}$ as above.
- Let $I_{\mathscr{S}_K/K_\infty}(x, t_1, \ldots, t_k)$ and $u_{\mathscr{S}_K/K_\infty}$ be as in Notation 3.9. (Such a polynomial and a rational constant exist by Corollary 3.8 given our assumptions on primes dividing the degrees of subextensions of K_∞.)
- Let $O_{K_\infty,\mathscr{W}_{K_\infty}}, O_{K_\infty,\mathscr{S}_{K_\infty}}$ be the integral closures of $O_{K,\mathscr{W}_K}$ and $O_{K,\mathscr{S}_K}$ in K_∞ respectively (or alternatively one can think of $\mathscr{W}_{K_\infty}$ and $\mathscr{S}_{K_\infty}$ as being the set of prime ideals of the ring of integers of K_∞ containing all the prime ideals $\mathfrak{p}$ such that $\mathfrak{p} \cap K \in \mathscr{W}_K$ or $\mathfrak{p} \cap K \in \mathscr{S}_K$ respectively).
- Let $B < l_0 < l_1 < \ldots < l_{h_{LE_1}p_2} \in \mathbb{Z}_{>0}$ be a set of positive integers such that the set of polynomials $\{Q(X + l_i), i = 0, \ldots, h_{LE_1}p_2\}$ is linearly independent over $\mathbb{C}$. (Such a set of positive integers exists by Lemma 12.1 and the constant B is defined in Notation 6.8.)
- Let γ_{E_1}, γ_L generate E_1 and L over $\mathbb{Q}$.
- Let C be a constant defined in Lemma 4.1 of [30].

The following proposition contains the technical core of this section and is a slightly modification of Proposition 6.2 of [30].

Proposition 9.2. *Suppose the following set of equations is satisfied for all $i \in \{0, 1, \dots, h_{KLE_1}p_2\}$; some $t_1, \dots, t_k \in K_\infty, y, x_i, y_i \in O_{K_\infty, \mathscr{W}_{K_\infty}}; \bar{\nu}, \nu, \bar{\lambda}_i, \lambda_i, \bar{\varepsilon}, \varepsilon_i, w_i, z_i, a_i, Z_i, W_i \in O_{K_\infty, \mathscr{W}_{K_\infty}}[\gamma_L, \gamma_{E_1}]$.*

$$\begin{cases} \mathbf{N}_{K_\infty E_1 L/LK_\infty}(\bar{\nu}) = 1, \\ \mathbf{N}_{K_\infty E_1 L/EK_\infty}(\bar{\nu}) = 1, \\ \bar{\nu} \neq \pm 1, \\ \nu = \bar{\nu}^{2h_{LE_1}} \end{cases} \tag{9.1}$$

$$\begin{cases} \mathbf{N}_{K_\infty E_1 L/LK_\infty}(\bar{\lambda}_i) = 1, \\ \mathbf{N}_{K_\infty E_1 L/EK_\infty}(\bar{\lambda}_i) = 1, \\ \bar{\lambda}_i \neq \pm 1, \\ \lambda_i = \bar{\lambda}_i^{2h_{LE_1}}, \end{cases} \tag{9.2}$$

$$\begin{cases} \mathbf{N}_{K_\infty E_1 L/LK_\infty}(\bar{\varepsilon}_i) = 1, \\ \mathbf{N}_{K_\infty E_1 L/E_1K_\infty}(\bar{\varepsilon}_i) = 1, \\ \bar{\varepsilon}_i \neq \pm 1, \\ \varepsilon_i = \bar{\varepsilon}_i^{2h_{LE_1}}, \end{cases} \tag{9.3}$$

$$\lambda_i - 1 = (\nu - 1)z_i, \tag{9.4}$$

$$\varepsilon_i - 1 = (\nu - 1)w_i, \tag{9.5}$$

$$x_i - z_i = (\nu - 1)Z_i \tag{9.6}$$

$$\nu - 1 = x_i^2 a_i, \tag{9.7}$$

$$x_i = Q(u_{\mathscr{S}_K/K_\infty} y + l_i), \tag{9.8}$$

$$y_i = x_i^{h_{LE_1}}, \tag{9.9}$$

$$I_{\mathscr{S}_K/K_\infty}(y, t_1, \dots, t_k) = 0, \tag{9.10}$$

$$|\sigma(y_i)| > 1, \forall \sigma : K_\infty \to \mathbb{C}, \tag{9.11}$$

$$y_i - w_i = y_i^{2A} C D W_i. \tag{9.12}$$

Then $y \in O_{K, \mathscr{W}_K}$.

Conversely, if $y \in \mathbb{Z}_{>0}$, then these equations can be satisfied for all $i \in \{0, 1, \dots, h_{KLE_1}p_2\}$; some $t_1, \dots, t_k \in K, y, x_i, y_i \in O_{K, \mathscr{W}_K}; \bar{\nu}, \nu, \bar{\lambda}_i, \lambda_i, \bar{\varepsilon}, \varepsilon_i, w_i, z_i, a_i, Z_i, W_i \in O_{K, \mathscr{W}_K}[\gamma_L, \gamma_{E_1}]$.

Proof. Suppose all the equations are satisfied with variables as indicated in the statement of the proposition. Let $\hat{M} \subset K_\infty$ be the smallest overfield of K such that for all $i \in \{0, 1, \dots, h_{LE_1}p_2\}$ we have that $t_1, \dots, t_k \in \hat{M}, y, x_i, y_i \in O_{\hat{M}, \mathscr{W}_{\hat{M}}}, \bar{\nu}, \nu, \bar{\lambda}_i, \lambda_i, \bar{\varepsilon}, \varepsilon_i, w_i, z_i \in O_{\hat{M}, \mathscr{W}_{\hat{M}}}[\gamma_{E_1}, \gamma_L]$. If $K \neq K(y) = M \subseteq \hat{M}$, then let $\bar{M}$ be a proper subfield of $\hat{M}$ satisfying the conditions in the Notation and Assumptions 9.1.

Since, by assumption for any subfield M of K_∞ such that M contains K we have that $[ME_1 : M] = p_1$ and $[ML : M] = 2$ we conclude that γ_{E_1} and γ_L have the same conjugates over LK_∞ and E_1K_∞ respectively as over $L\hat{M}$ and $E_1\hat{M}$ respectively, and therefore we can rewrite the equations (9.1)– (9.3) as

$$\begin{cases} \mathbf{N}_{\hat{M}E_1L/L\hat{M}}(\bar{\nu}) = 1, \\ \mathbf{N}_{\hat{M}E_1L/E_1\hat{M}}(\bar{\nu}) = 1, \\ \bar{\nu} \neq \pm 1, \\ \nu = \bar{\nu}^{2h_{LE_1}} \end{cases} \tag{9.13}$$

$$\begin{cases} \mathbf{N}_{\hat{M}E_1L/L\hat{M}}(\bar{\lambda}_i) = 1, \\ \mathbf{N}_{\hat{M}E_1L/E_1\hat{M}}(\bar{\lambda}_i) = 1, \\ \bar{\lambda}_i \neq \pm 1, \\ \lambda_i = \bar{\lambda}_i^{2h_{LE_1}}, \end{cases} \tag{9.14}$$

$$\begin{cases} \mathbf{N}_{\hat{M}E_1L/L\hat{M}}(\bar{\varepsilon}_i) = 1, \\ \mathbf{N}_{\hat{M}E_1L/E_1\hat{M}}(\bar{\varepsilon}_i) = 1, \\ \bar{\varepsilon}_i \neq \pm 1, \\ \varepsilon_i = \bar{\varepsilon}_i^{2h_{LE_1}}, \end{cases} \tag{9.15}$$

Now from Lemma 4.2 we conclude that ν, λ_i and ε_i for all $i \in \{0, 1, \ldots, h_{LE_1}p_2\}$ are in $O_{E_1L,\mathscr{W}_{E_1L}}$. Thus, $z_i, w_i \in O_{E_1L,\mathscr{W}_{E_1L}}$ for all $i \in \{0, 1, \ldots, h_{LE_1}p_2\}$ as well. Note also that since $y_i \in M$, and $\nu, z_i, w_i \in E_1L$ we have that $Z_i, W_i \in MLE_1$ by equations (9.6) and (9.12) respectively. In other words, (9.6)– (9.9) hold over ME_1L. Further, while (9.10) a priori might hold over a bigger field, its implication about lack of factors of primes in $\mathscr{W}_M$ in the numerator of the divisor of x_i hold over ME_1L. Similarly, (9.11) also holds over M.

Given the discussion above, by Lemma 5.1 of [30], using equations (9.6)–(9.10), we now conclude that $y_i = x_i^{h_{LE_1}} = u_i\delta_i^{-1}$, where $u_i \in O_{KLE}$, $\delta_i \in O_{MLE}$ and all the primes in the divisor of δ_i are in $\mathscr{W}_{MLE_1}$. Proceeding further, by a slight modification of Lemma 5.2 of [30] we obtain from equation (9.12) that $y_i \in \bar{M}LE_1$. (In Lemma 5.2 of [30] we had that $w_i, W_i \in M$ and $w_i \in K$ instead of MLE_1 and LE_1 respectively, and the conclusion is that $y_i \in \bar{M}$. However, the argument is the same for our case.) Since $y_i \in M$ and M and LE_1 are linearly disjoint over $\bar{M}$, we conclude that $y_i \in M \cap \bar{M}LE_1 = \bar{M}$. The final step is to note that for all i we have that $y_i = (Q(u_{\mathscr{S}_K}y + l_i))^{h_{LE_1}} \in \mathbb{Z}[y]$, where and $(Q(u_{\mathscr{S}_K}y + l_i))^{h_{LE_1}}$ is of degree $h_{LE_1p_2}$. Thus, if $y_0, \ldots, y_{h_{LE_1}p_2} \in \bar{M}$, then by Lemma 5.1 of [25], it is the case that $y \in \bar{M}$ and therefore actually $y \in K$.

Now the satisfiability assertion can be shown in exactly same fashion as it was done in Proposition 6.2 of [30]. We should note only that given our choice of l_i's, we can satisfy the equations above for any positive integer y. □

Before we state the main result of this section, we need to revisit some old number field results.

Theorem 9.3. *There exists a set $\hat{\mathscr{W}}_K$ of primes of K such that $\hat{\mathscr{W}}_K \setminus \mathscr{W}_K = \{\mathfrak{t}_1, \ldots, \mathfrak{t}_r\}$ is a finite set, no $\mathfrak{t}_i$ lies above a rational prime ramified in K_∞, and $O_{K,\hat{\mathscr{W}}_K} \cap \mathbb{Q}$ has a Diophantine definition over $O_{K,\mathscr{W}_K}$.*

Proof. Let K_G be the Galois closure of K over $\mathbb{Q}$. Note that due to Notation and Assumption 4.1 we have that $([K_G : K], p_2) = 1$ and therefore μ is of degree p_2 over K_G. Let $F_1, \ldots, F_k$ be all the cyclic subextensions of K_G. By Lemma 12.5, for each i there are infinitely many K_G-primes $\mathfrak{T}_i$ such that each $\mathfrak{T}_i$ lies above a F_i-prime not splitting in the extension K_G/T_i and each $\mathfrak{T}_i$ splits completely in E_2/F_i. We claim that by Theorem 2.2 of [28] we have that $O_{K_G,\mathscr{W}_{K_G}\cup\{\mathfrak{T}_1,\ldots,\mathfrak{T}_r\}} \cap \mathbb{Q}$ has a Diophantine definition over $O_{K_G,\mathscr{W}_{K_G}\cup\{\mathfrak{T}_1,\ldots,\mathfrak{T}_r\}}$. If we compare our data to the data in Theorem 2.2 of [28], we will see that we seem to be out of compliance on two points. First of all we need an element γ with $\gamma^2 \in K_G$ such that $K_G(\gamma)$ is totally complex and all $\mathfrak{T}_i$ split in the extension $K_G(\gamma)/K_G$. By the Weak Approximation Theorem we can find $b \in K_G$ such that all the conjugates of b over $\mathbb{Q}$ are negative and $b \equiv 1 \mod \prod_{i=1}^r \mathfrak{T}_i$. If we choose a complex number γ satisfying $\gamma^2 = b$, then $K_G(\gamma)$ will satisfy the requirements by Proposition 25 of Section 8, Chapter I and Proposition 16, Section 3, Chapter III of [9]. The other part out of compliance is the

potential presence of finitely many primes in $\mathscr{W}_{K_G}$ dividing the discriminant of the power basis of μ over K_G. We take care of this problem by using Proposition 2.2.

Now let $\{\mathfrak{t}_1, \ldots, \mathfrak{t}_r\}$ be the set of K-primes lying below $\{\mathfrak{T}_1, \ldots, \mathfrak{T}_r\}$. Let $\hat{\mathscr{W}}_K = \mathscr{W}_K \cup \{\mathfrak{t}_1, \ldots, \mathfrak{t}_r\}$ and let $\hat{W}_{K_G}$ be the set of all K_G-primes lying above $\hat{W}_K$ primes. Observe that $O_{K_G, \hat{\mathscr{W}}_{K_G}}$ is the integral closure of $O_{K, \hat{\mathscr{W}}_K}$ in K_G and $\hat{\mathscr{W}}_{K_G} \setminus (\mathscr{W}_{K_G} \cup \{\mathfrak{T}_1, \ldots, \mathfrak{T}_r\})$ is a finite set. (The extra primes are other factors of $\mathfrak{t}_i$'s in K_G.) Using what we know about $O_{K_G, \mathscr{W}_{K_G} \cup \{\mathfrak{T}_1, \ldots, \mathfrak{T}_r\}}$ and Proposition 2.2 again we can assert that $O_{K_G, \hat{\mathscr{W}}_{K_G}} \cap \mathbb{Q}$ has a Diophantine definition over $O_{K_G, \hat{\mathscr{W}}_{K_G}}$. Finally, by Proposition 2.6, we finally conclude that $O_{K, \hat{\mathscr{W}}_K} \cap \mathbb{Q}$ has a Diophantine definition over $O_{K, \hat{\mathscr{W}}_K}$. □

We are now ready for the main theorem of this section.

Theorem 9.4. (1) *There exist a positive integer n and a polynomial $F(t, \bar{x}) \in K[t, \bar{x}]$ satisfying the following conditions. For any $t \in O_{K_\infty, \mathscr{W}_{K_\infty}}$, if there exists $\bar{x} \in (O_{K_\infty, \mathscr{W}_{K_\infty}})^n$ such that $F(t, \bar{x}) = 0$, then $t \in O_{K, \mathscr{W}_K}$. Further, if $t \in O_{K, \mathscr{W}_K}$, there exist $\bar{x} \in (O_{K, \mathscr{W}_K})^n$ such that $F(t, \bar{x}) = 0$. Thus, $O_{K, \mathscr{W}_K}$ is existentially definable over $O_{K_\infty, \mathscr{W}_{K_\infty}}$.*

(2) *There exists a set of K-primes $\hat{\mathscr{W}}_K$, a positive integer n, and a polynomial $F(t, \bar{x}) \in K[t, \bar{x}]$ satisfying the following conditions.*
   (a) *$\hat{\mathscr{W}}_K \setminus \mathscr{W}_K$ is a finite set.*
   (b) *For any $t \in O_{K_\infty, \hat{\mathscr{W}}_{K_\infty}}$, where $O_{K_\infty, \hat{\mathscr{W}}_{K_\infty}}$ is the integral closure of $O_{K, \hat{\mathscr{W}}_K}$ in K_∞, if there exists $\bar{x} \in (O_{K_\infty, \hat{\mathscr{W}}_{K_\infty}})^n$ such that $F(t, \bar{x}) = 0$, then $t \in O_{K_\infty, \hat{\mathscr{W}}_{K_\infty}} \cap \mathbb{Q}$. Further, if $t \in O_{K_\infty, \hat{\mathscr{W}}_{K_\infty}} \cap \mathbb{Q}$, there exist $\bar{x} \in (O_{K, \hat{\mathscr{W}}_K})^n$ such that $F(t, \bar{x}) = 0$.*
   (c) *$O_{K_\infty, \hat{\mathscr{W}}_{K_\infty}} \cap \mathbb{Q}$ is existentially definable over $O_{K_\infty, \mathscr{W}_{K_\infty}}$.*

(3) *There exists a positive integer n and a polynomial $F(t, \bar{x}) \in K[t, \bar{x}]$ satisfying the following conditions. For any $t \in O_{K_\infty, \mathscr{S}_{K_\infty}}$, if there exists $\bar{x} \in (O_{K_\infty, \mathscr{S}_{K_\infty}})^n$ such that $F(t, \bar{x}) = 0$, then $t \in O_{K_\infty, \mathscr{S}_{K_\infty}} \cap \mathbb{Q}$. Further, if $t \in O_{K_\infty, \mathscr{S}_{K_\infty}} \cap \mathbb{Q}$, there exist $\bar{x} \in (O_{K, \mathscr{S}_K})^n$ such that $F(t, \bar{x}) = 0$. Thus, $O_{K_\infty, \mathscr{S}_{K_\infty}} \cap \mathbb{Q}$ is existentially definable over $O_{K_\infty, \mathscr{S}_{K_\infty}}$.*

Proof. Most of the work for the proof of the first assertion has already been done in Proposition 9.2. We just have to note that by the discussion in Section 2, all the equations and conditions (9.1)–(9.12) can be rewritten as polynomial equations with coefficients in K and with the variables ranging in $O_{K_\infty, \mathscr{W}_{K_\infty}}$.

To show that the second assertion holds we need to show that $O_{K, \hat{\mathscr{W}}_K}$ is existentially definable over $O_{K_\infty, \hat{\mathscr{W}}_{K_\infty}}$, where following the notational scheme used so far, $O_{K_\infty, \hat{\mathscr{W}}_{K_\infty}}$ is the integral closure of $O_{K, \hat{\mathscr{W}}_K}$ in K_∞. Now by Theorem 9.3, we can assume that the new primes allowed in the denominators of divisors are not ramified in K_∞. Thus, we can use the fact that we can define integrality at such primes to obtain the requisite existential definition. More precisely, let $F(t, \bar{x})$ be the polynomial from the first assertion of the theorem. Let $\mathscr{T}_K = \{\mathfrak{t}_1, \ldots, \mathfrak{t}_k\}$ and let $I_{\mathscr{T}_K / K_\infty}(x, t_1, \ldots, t_k)$ be defined as in Notation 3.9. Given the choice of primes in $\mathscr{T}_K$, we can take $u_{\mathscr{T}_K / K_\infty} = 1$. Next consider the following system of equations

$$\left\{ \begin{array}{c} F(t, \bar{x}) = 0 \\ I_{\mathscr{T}_K / K_\infty}(t, w_1, \ldots, w_k) = 0 \\ I_{\mathscr{T}_K / K_\infty}(x_1, w_{1,1}, \ldots, w_{1,k}) = 0 \\ \cdots \end{array} \right. \tag{9.16}$$

Suppose this system has solutions in $O_{K_\infty, \hat{\mathscr{W}}_{K_\infty}}$. Then $F(t, \bar{x}) = 0$ has solutions in $O_{K_\infty, \mathscr{W}_{K_\infty}}$ and $t \in O_{K, \mathscr{W}_K}$. Conversely, if $t \in O_{K, \mathscr{W}_K}$, then $F(t, \bar{x}) = 0$ has solutions in $O_{K, \mathscr{W}_K}$ and we can find solutions to $I_{\mathscr{T}_K / K_\infty}(t, w_1, \ldots, w_k) = 0, I_{\mathscr{T}_K / K_\infty}(x_1, w_{1,1}, \ldots, w_{1,k}) = 0, \ldots$ in K also.

To show that the third assertion is true recollect that $\mathbb{Z}$ is existentially definable over $O_{K, \mathscr{S}_K}$ by results of Denef and Proposition 2.2, and since the primes of $\mathscr{S}_K$ are the only primes which *have* to be contained in $\mathscr{W}_K$ in order for the arguments to go through (i.e. to have solutions to the norm equations in the rings under consideration), the first assertion of the theorem implies the third one.

□

10. Diophantine Definability and Decidability in the Integral Closure of Big and Small Subrings of Extensions of Degree 2 of Totally Real Algebraic Extensions of $\mathbb{Q}$.

In this section we consider the definability for the extensions of degree 2 when the underlying totally real field possibly has an infinite degree over $\mathbb{Q}$.

Notation and Assumptions 10.1. We start again with adding to notation and assumptions we have used so far. We continue to think of M as ranging over all subextensions of K_∞ containing K with all the preceding assumptions (i.e assumption in Assumptions and Notation 4.1, 5.1, 6.1, 7.1, 9.1) holding for any such M.

- Let $\mathscr{M}_K$ be the set of primes of K not splitting in the extension G/K.
- Let $\mathscr{N}_K$ be the set of K-primes not splitting in the extension E_1E_2G/K. We will assume that $\mathscr{N}_K \subset \mathscr{M}_K \cap \mathscr{V}_K \subset \mathscr{Z}_K$. Let $\mathscr{A}_K = \mathscr{N}_K \cup \mathscr{S}_K$. Given our assumptions we also have that $\mathscr{A}_K \subset \mathscr{U}_K \cap \mathscr{W}_K$.
- Let $\mathscr{L}_K$ be formed by removing the highest degree prime of K from every complete set of $\mathbb{Q}$-conjugates in $\mathscr{N}_K$.
- Let $\mathscr{R}_K = \mathscr{L}_K \cup \mathscr{S}_K$.
- Let $G_\infty = K_\infty(\alpha) = GK_\infty, H_\infty = K_\infty(\delta) = HK_\infty$.
- Let $O_{G_\infty,\mathscr{R}_{G_\infty}}$ be the integral closure of $O_{K,\mathscr{R}_K}$ in G_∞.
- Assume that either any root of unity in E_2GHK_∞ is already in G_∞ or the group of roots of unity of E_2GHK_∞ is finite. In the first case set $m = 2$, in the second case let m be a multiple of the size of the group of roots of unity of $EGHK_\infty$.
- Let $O_{K_\infty,\mathscr{U}_{K_\infty}}, O_{G_\infty,\mathscr{U}_{G_\infty}}$ be the integral closures of $O_{K,\mathscr{U}_K}$ and $O_{G,\mathscr{U}_G}$ respectively.
- Let $O_{G_\infty,\mathscr{R}_{G_\infty}}$ be the integral closure of $O_{K,\mathscr{R}_K}$ in G_∞.
- Let $O_{K_\infty,\mathscr{S}_{K\infty}}, O_{G_\infty,\mathscr{S}_{G_\infty}}$ be the integral closures of $O_{K,\mathscr{S}_K}$ in K_∞ and G_∞ respectively.

We will separate the following assumption from the rest, since we will not be using it all the time. We will specify explicitly where this assumption is used.

Assumptions 10.2.
- For all number fields M as above we have that $[M : K]$ is odd.

Lemma 10.3. *Suppose Assumption 10.2 holds. Then the primes in $\mathscr{M}_M$ do not split in the extension GE_2M/M, i.e. this notation use is consistent with Notation and Assumption 4.1 and 6.1.*

Proof. Given Assumption 10.2, we have that $([M : K], [GE_2 : K]) = 1$ and therefore we can apply Lemmas 12.4 and 12.6 of the Appendix to reach the desired conclusion. □

The following lemma also follows from the consideration of the degrees of the extension.

Lemma 10.4. *The primes of $\mathscr{Z}_G$ do not split in the extension E_2G/G.*

Proposition 10.5. *Under Assumption 10.2 we have that $O_{G_\infty,\mathscr{U}_{G_\infty}}$ contains a Diophantine subset* B *satisfying the following conditions:*

(1) *If $x \in$ B, then $x \in O_{K_\infty,\mathscr{U}_{K_\infty}}$.*
(2) *If $x \in O_{K,\mathscr{U}_K}$, then $x \in$ B.*

Alternatively, we can say that there exists a polynomial $P(t, X_1, \ldots, X_l)$ with coefficients in K, such that

$$\forall t, X_1, \ldots, X_n \in O_{G_\infty,\mathscr{U}_{G_\infty}} : T_{\mathscr{U}}(t, X_1, \ldots, X_n) = 0 \Longrightarrow t \in K_\infty \cap O_{G_\infty,\mathscr{U}_{G_\infty}}, \tag{10.1}$$

and

$$\forall t \in K, \exists X_1, \ldots, X_n \in O_{K,\mathscr{U}_K} : T_{\mathscr{U}}(t, X_1, \ldots, X_n) = 0, \tag{10.2}$$

Proof. The proof will use Proposition 7.3 as its foundation. However we have to adjust somewhat the equations used in that proposition. First of all we change the initial range of values for the variables. Let $x_0, x_1 \in O_{G_\infty,\mathscr{U}_{G_\infty}}, a_1, a_2, b_1, b_2, u, v \in O_{G_\infty,\mathscr{U}_{G_\infty}}[\mu]$, $\varepsilon_i \in O_{G_\infty,\mathscr{U}_{G_\infty}}[\mu, \delta], i = 1, \ldots, 4, t_1, \ldots, t_k \in G_\infty$ and assume the following conditions and equations are satisfied.

$$I_{\mathscr{E}_K/G_\infty}(x_0, t_1, \ldots, t_k) = 0, \tag{10.3}$$

$$x_1 = Q(u_{\mathscr{E}_K/G_\infty} x_0), \tag{10.4}$$

$$\begin{cases} \mathbf{N}_{E_2HG_\infty/E_2G_\infty}(\varepsilon_i) = 1, i = 1, \dots, 4, \\ \mathbf{N}_{E_2HG_\infty/HG_\infty}(\varepsilon_i) = 1, i = 1, \dots, 4, \end{cases} \tag{10.5}$$

$$\gamma_i = \varepsilon_i^m, i = 1, \dots, 4, \tag{10.6}$$

$$\frac{\gamma_{2j} - 1}{\gamma_{2j-1} - 1} = a_j - \delta b_j, j = 1, 2 \tag{10.7}$$

$$\gamma_i = c_i + \delta d_i, i = 1, \dots, 4, \tag{10.8}$$

$$1 \leq |\sigma(x_1)| \leq Q(B + \sigma(a_1^2 - db_1^2)^2), \tag{10.9}$$

where σ ranges over all real embedding of E_2G_∞ into $\tilde{\mathbb{Q}}$,

$$x_1 - (a_2 - \delta b_2) = (c_3 + \delta d_3)(u + v\delta), \tag{10.10}$$

$$Pax_1Q(B + (a_1^2 - db_1^2)^2) \big| (c_3 - 1 + \delta d_3), \tag{10.11}$$

where P is defined as in Proposition 7.3 and $I_{\mathscr{E}_K/G_\infty}, u_{\mathscr{E}_K/G_\infty}$ as in Notation 3.9. (We remind the reader that the polynomial $I_{\mathscr{E}_K/G_\infty}$ exists by Corollary 3.8 and we can choose $u_{\mathscr{E}_K/G_\infty} \in \mathbb{Z}_{>0}$.) Then, we claim, $x_1 \in K_\infty$.

Conversely, we claim that if $x_0 \in \mathbb{Z}_{>0}$, the conditions and equations above can be satisfied with $a_1, a_2, b_1, b_2, u, w \in O_{K,\mathscr{U}_K}[\mu]$, $\varepsilon_i \in O_{K,\mathscr{U}_K}[\mu, \delta], i = 1, \dots, 4$, and $t_1, \dots, t_k \in K$.

To prove the first claim, observe the following. Let M such that GHE_2M contains $\alpha, \delta, \mu, x_0, a_1, a_2, b_1, b_2$, $u, v, \varepsilon_i, t_1, \dots, t_k$. Then given our assumptions on the fields under consideration, in the equations above we can replace E_2HG_∞ by GE_2HM, $G_\infty E_2$ by GE_2M, and finally K_∞ by M, while the equalities and other conditions will continue to be true, assuming we modify the prime sets by choosing the primes in the finite extensions which are below $\mathscr{U}_{G_\infty}$. Then we can use Proposition 7.3 to reach the conclusion that $x_1 \in M \subset K_\infty$. The converse claim follows directly from Proposition 7.3.

The only remaining issue is being able to rewrite all the equations and conditions as polynomial equations with variables taking values in G_∞, and also observe that we can require $x_0 + 1, \dots, x_0 + p_2$ to satisfy the equations above. Here we can proceed exactly as in Proposition 8.1. □

Remark 10.6. Let $\hat{\mathscr{U}}_K$ be a subset of primes of K such that $\hat{\mathscr{U}}_K \setminus \mathscr{U}_K$ is a finite set containing no factors of rational primes ramified in G_∞. Then by Corollary 3.8 the statement of the proposition above will apply to $O_{G_\infty,\hat{\mathscr{U}}_{G_\infty}}$ – the integral closure of $O_{K,\hat{\mathscr{U}}_K}$.

We now specialize the proposition above for "small" rings. Please note that we *do not need* Assumption 10.2 below.

Corollary 10.7. *$O_{G_\infty,\mathscr{S}_{G_\infty}}$ contains a Diophantine subset* B *satisfying the following conditions:*

1. *If $x \in$ B, then $x \in O_{K_\infty,\mathscr{S}_\infty}$.*
2. *If $x \in O_{K,\mathscr{S}_K}$, then $x \in$ B.*

or alternatively, we can say that there exists a polynomial $T_{\mathscr{S}}(t, X_1, \dots, X_l)$ with coefficients in K, such that

$$\forall t, X_1, \dots, X_n \in O_{G_\infty,\mathscr{S}_\infty} : T_{\mathscr{S}}(t, X_1, \dots, X_n) = 0 \Longrightarrow t \in K_\infty \cap O_{G_\infty,\mathscr{S}_\infty}, \tag{10.12}$$

and

$$\forall t \in K, \exists X_1, \dots, X_n \in O_{K,\mathscr{S}_K} : T_{\mathscr{S}}(t, X_1, \dots, X_n) = 0, \tag{10.13}$$

We can now combine the results above with Theorem 9.4 to obtain the results below. Observe that we now need the "majority" of K-primes not splitting in E_1/K or E_2/K. The analogous requirements should also hold for primes in the extensions of K. This leads us to use $\mathscr{A}_K$ as the set of the allowed denominators.

Theorem 10.8. (1) *Assume Assumption 10.2 holds. Then there exist a positive integer n and a polynomial $F(t,\bar{x}) \in K[t,\bar{x}]$ satisfying the following conditions. For any $t \in O_{G_\infty,\mathscr{A}_{G_\infty}}$, if there exists $\bar{x} \in (O_{G_\infty,\mathscr{A}_{G_\infty}})^n$ such that $F(t,\bar{x}) = 0$, then $t \in O_{K,\mathscr{A}_K}$. Further, if $t \in O_{K,\mathscr{A}_K}$, there exist $\bar{x} \in (O_{K,\mathscr{A}_K})^n$ such that $F(t,\bar{x}) = 0$. Thus, $O_{K,\mathscr{A}_K}$ is existentially definable over $O_{G_\infty,\mathscr{A}_{G_\infty}}$.*

(2) *Assume Assumption 10.2 holds. Then there exists a set of K-primes $\hat{\mathscr{A}}_K$, a positive integer n, and a polynomial $F(t,\bar{x}) \in K[t,\bar{x}]$ satisfying the following conditions.*
   (a) *$\hat{\mathscr{A}}_K \setminus \mathscr{A}_K$ is a finite set.*
   (b) *For any $t \in O_{G_\infty,\hat{\mathscr{A}}_{G_\infty}}$, where $O_{G_\infty,\hat{\mathscr{A}}_{G_\infty}}$ is the integral closure of $O_{K,\hat{\mathscr{A}}_K}$ in G_∞, if there exists $\bar{x} \in (O_{G_\infty,\hat{\mathscr{A}}_{G_\infty}})^n$ such that $F(t,\bar{x}) = 0$, then $t \in O_{K_\infty,\hat{\mathscr{A}}_{K_\infty}} \cap \mathbb{Q}$. Further, if $t \in O_{G_\infty,\hat{\mathscr{A}}_{G_\infty}} \cap \mathbb{Q}$, there exist $\bar{x} \in (O_{K,\hat{\mathscr{A}}_K})^n$ such that $F(t,\bar{x}) = 0$.*
   (c) *$O_{G_\infty,\hat{\mathscr{A}}_{G_\infty}} \cap \mathbb{Q}$ is existentially definable over $O_{G_\infty,\mathscr{A}_{G_\infty}}$.*

(3) *Assume Assumption 10.2 holds. Then there exists a set of K-primes $\hat{\mathscr{R}}_K$, a positive integer n, and a polynomial $F(t,\bar{x}) \in K[t,\bar{x}]$ satisfying the following conditions.*
   (a) *$\hat{\mathscr{R}}_K \setminus \mathscr{R}_K$ is a finite set.*
   (b) *For any $t \in O_{G_\infty,\hat{\mathscr{R}}_{G_\infty}}$, where $O_{G_\infty,\hat{\mathscr{R}}_{G_\infty}}$ is the integral closure of $O_{K,\hat{\mathscr{R}}_K}$ in G_∞, if there exists $\bar{x} \in (O_{G_\infty,\hat{\mathscr{R}}_{G_\infty}})^n$ such that $F(t,\bar{x}) = 0$, then $t \in O_{G_\infty,\hat{\mathscr{R}}_{G_\infty}} \cap \mathbb{Q}$. Further, if $t \in O_{G_\infty,\hat{\mathscr{R}}_{G_\infty}} \cap \mathbb{Q}$, there exist $\bar{x} \in (O_{K,\hat{\mathscr{R}}_K})^n$ such that $F(t,\bar{x}) = 0$.*
   (c) *$O_{G_\infty,\hat{\mathscr{R}}_{G_\infty}} \cap \mathbb{Q}$ is existentially definable over $O_{G_\infty,\mathscr{R}_{G_\infty}}$.*
   (d) *$\mathbb{Z}$ is existentially definable over $O_{G_\infty,\hat{\mathscr{R}}_{G_\infty}}$ and therefore HTP is undecidable over $O_{G_\infty,\hat{\mathscr{R}}_{G_\infty}}$.*

(4) *There exists a positive integer n and a polynomial $F(t,\bar{x}) \in K[t,\bar{x}]$ satisfying the following conditions. For any $t \in O_{G_\infty,\mathscr{S}_{G_\infty}}$, if there exists $\bar{x} \in (O_{G_\infty,\mathscr{S}_{G_\infty}})^n$ such that $F(t,\bar{x}) = 0$, then $t \in O_{G_\infty,\mathscr{S}_{G_\infty}} \cap \mathbb{Q}$. Further, if $t \in O_{G_\infty,\mathscr{S}_{K_\infty}} \cap \mathbb{Q}$, there exist $\bar{x} \in (O_{K,\mathscr{S}_K})^n$ such that $F(t,\bar{x}) = 0$. Thus, $O_{G_\infty,\mathscr{S}_{G_\infty}} \cap \mathbb{Q}$ and $\mathbb{Z}$ are is existentially definable over $O_{G_\infty,\mathscr{S}_{G_\infty}}$, and HTP is not decidable over this ring.*

Proof. The only point which requires clarification is the definability of $\mathbb{Z}$ over $O_{G_\infty,\mathscr{R}_{G_\infty}}$. Here we just point out that by construction, $O_{G_\infty,\mathscr{R}_{G_\infty}} \cap \mathbb{Q}$ is a "small" subring of $\mathbb{Q}$, and by Proposition 2.2 we know that $\mathbb{Z}$ is definable in "small" subrings of $\mathbb{Q}$. □

The main drawback of the results above is that the numerous conditions make it unclear if any "nice" (or for that matter any) class of infinite algebraic extensions of $\mathbb{Q}$ is covered by the theorems. In the final section of the paper we will show that infinite cyclotomics with finitely many ramified rational primes, and consequently all the abelian extensions embedded in them, satisfy the assumptions of our propositions.

11. **Infinite Cyclotomic and Abelian Extensions.**

To begin with we revisit the issue we have investigated in [30] and [24]. This issue concerns the number of factors a rational prime can have in a in infinite cyclotomic extension. This matter was investigated in [30] using an elementary argument. Unfortunately, it was done for odd primes only which is not sufficient for our current purposes.

Notation 11.1. We add the following notation.

- Let $\{q_1,\dots,q_k\}$ be a finite set of rational primes.
- For $i = 1,\dots,k$ and any positive integer j, let $\xi_{i,j}$ be a primitive q_i^j-th root of unity.
- We specialize K_∞ to be the largest totally real subfield of $G_\infty = \mathbb{Q}(\{\xi_{i,j}, i = 1,\dots,k, j \in \mathbb{Z}_{>0}\})$.
- We now let $M \subset K_\infty$ range over number fields contained in K_∞. We also vary K across subfields of K_∞ while preserving the assumption that $K \subset M$.
- For a rational number p, let $g_p(M)$ be the number of factors p has in M. Let $g_p(K_\infty) = \max_M\{g_p(M)\}$.
- For a rational prime $p \notin \{q_1,\dots,q_k\}$, let n_i be the order of p modulo $q_i^{a_i}$, where $a_i = 1$ if q_i is odd, and $a_i = 2$ if $q_i = 2$. In other words, n_i is the smallest positive integer such that $p^{n_i} \equiv 1 \mod q_i^{a_i}$. Also, let $r_i = \mathrm{ord}_{q_i}(p^{n_i} - 1)$.

Lemma 11.2. *Let $x \in \mathbb{Z}$ and let q be a rational prime. Assume further that $ord_q(x-1) = n$, where n is a positive integer. If $q = 2$, we will assume that $n \geq 2$. Let $l \neq q$ be a prime number. Then $ord_q(x^l - 1) = n$ while $ord_q(x^q - 1) = n + 1$.*

Proof. Let x, q, n, l be as in the statement of the lemma and consider the factorization of $x^l - 1$ over $\mathbb{Q}(\mu_l)$ where μ_l is a primitive l-th root of unity,

$$x^l - 1 = (x-1)(x-\mu_l)(x-\mu_l^2)\dots(x-\mu^{l-1})$$

Let $\mathfrak{q}$ be a factor of q in $\mathbb{Q}(\mu_l)$, and observe that since $l \neq q$, we have that $\mathfrak{q}$ is not ramified over q. Thus, on the one hand,

$$\mathrm{ord}_q(x^l-1) = \mathrm{ord}_{\mathfrak{q}}(x^l-1) = \mathrm{ord}_{\mathfrak{q}}(x-1) + \sum_{j=1}^{l-1} \mathrm{ord}_{\mathfrak{q}}(x-\mu_l^j).$$

On the other hand, $\mathrm{ord}_{\mathfrak{q}}(x-\mu_l^j) = \min(\mathrm{ord}_{\mathfrak{q}}(x-1), \mathrm{ord}_{\mathfrak{q}}(1-\mu_l^j)) = 0$, since the only factor occurring in the divisor of $1-\mu_q^j$ is the factor of l.

Next consider the factorization of $x^q - 1$ in $\mathbb{Q}(\mu_q)$, where μ_q is a primitive q-th root of unity.

$$x^q - 1 = (x-1)(x-\mu_q)\dots(x-\mu_q^{q-1}),$$

Let $\mathfrak{q}$ be the ramified factor of q in this extension. Then $\mathrm{ord}_{\mathfrak{q}}(1-\mu_q^j) = 1$ for $j = 1, \dots, q-1$ and, given our assumptions for the case of $q = 2$, we have that $\mathrm{ord}_{\mathfrak{q}}(1-\mu_q^j) < \mathrm{ord}_{\mathfrak{q}}(x-1)$.

$$\begin{aligned}\mathrm{ord}_{\mathfrak{q}}(x^q-1) = n(q-1) + \sum_{j=1}^{q-1} \mathrm{ord}_q(x-\mu_q^j) &= n(q-1) + \sum_{j=1}^{q-1} \min(\mathrm{ord}_{\mathfrak{q}}(x-1), \mathrm{ord}_{\mathfrak{q}}(1-\mu_p^j)) \\ &= n(q-1) + (q-1) = (n+1)(q-1).\end{aligned}$$

Hence,

$$\mathrm{ord}_q(x^q-1) = \frac{\mathrm{ord}_{\mathfrak{q}}(x^q-1)}{q-1} = n+1.$$

□

From this lemma it immediately follows that the following statement is true.

Corollary 11.3. *For any $i = 1, \dots, k$ and any integers $l \geq 0$, $s > 0$, we have that $ord_{q_i}(p^s - 1) \geq r_i + l$ if and only if $s \equiv 0 \mod n_i p^l$.*

Using this corollary we can prove another consequence of Lemma 11.2.

Corollary 11.4. *Let $\{l_1, \dots, l_k\}$ be a set of non-negative numbers. Let $m = \prod_{i=1}^k q_i^{l_i + r_i}$. Let*

$$n = LCM(n_1 q_1^{l_1}, \dots, n_k q_k^{l_k}).$$

Then μ_m, a primitive m-th root of unity, is of degree n over $\mathbb{F}_p$ – a finite field of p elements.

Proof. Let F be a finite field of characteristic p. Let $p^s = |F|$. Then $\mu_m \in F$ if and only if $p^s - 1 \equiv 0 \mod m$. At the same time, by Corollary 11.3, we have that $p^s - 1 \equiv 0 \mod m$ if and only if $s \equiv 0 \mod n$, and thus the assertion of the corollary is true. □

Proposition 11.5. *Let p be a rational prime. Then $g_p(K_\infty) < \infty$.*

Proof. It is enough to show that the proposition holds for $\mathbb{Q}(\xi_{i,j}, i = 1, \dots, k, j \in \mathbb{Z}_{>0})$. We first consider the extension $\mathbb{Q}(\xi_i^{r_i + l_i}, i = 1, \dots, k)/\mathbb{Q}$, where, as above, $\{l_1, \dots, l_k\}$ is a set of non-negative integers. Let $\mathfrak{p}$ be a factor of p in this extension and let f be its relative degree. Since a power basis of a root of unity is always an integral basis over $\mathbb{Q}$, by Proposition 25 of Section 8, Chapter I of [9], to determine f, it is enough to determine the degree of ξ_m over $\mathbb{F}_p$, where m is as in Corollary 11.4. By Corollary 11.4, this degree is equal $LCM(q_1^{l_1} n_1, \dots, q_k^{l_k} n_k)$. Since p is not ramified in the extension $\mathbb{Q}(\xi_i^{r_i + l_i}, i = 1, \dots, k)/\mathbb{Q}$, we can conclude that the number of factors of p in $\mathbb{Q}(\xi_i^{r_i + l_i}, i = 1, \dots, k)$ is equal to $\dfrac{q_1^{r_1 + l_1 - 1}(q_1 - 1) \dots q_k^{r_k + l_k - 1}(q_k - 1)}{LCM(q_1^{l_1} n_1, \dots, q_k^{l_k} n_k)} \leq q_1^{r_1} \dots q_k^{r_k}$. □

Lemma 11.6. *Assuming that ramification degree of 2 is finite, there exists a number field $K \subset K_\infty$ such that for all number fields M with $K \subset M \subset K_\infty$ we have that $[M : K]$ is odd. Further the same assertion will be true for any finite extension of K in K_∞.*

Proof. Given our assumptions, without loss of generality, we can assume that

$$G_\infty = \mathbb{Q}(\xi_{1,r}, \{\xi_{i,j}, i = 2, \dots, k, j \in \mathbb{Z}_{>0}\}),$$

where $q_1 = 2$ and $r \in \mathbb{Z}_{>0}$. Let $G = \mathbb{Q}(\xi_{1,r}, \xi_{2,1}, \dots, \xi_{k,1})$. Then for any number field R with $G \subset R \subset G_\infty$, we have that $[R : G] = \prod_{i=2}^{k} q_i^{a_i}, a_i \in \mathbb{Z}_{\geq 0}$. Set K to be the largest totally real subfield of G and consider a number field $M \subset K_\infty$ with $K \subset M$. For some number field R, as above, we have that $[R : M] = 2$, and therefore by comparing degrees we can conclude that $[M : K] = [R : G]$ is an odd number. □

We now consider various other assumptions on K_∞ and G_∞ and prove the following proposition.

Proposition 11.7. *Let $K_0 \subset K_\infty$, and let $\mathscr{S}_{K_0}$ be a finite set of primes of K_0. Then for some infinite set $\mathscr{A}_{K_0}$ of K_0-primes containing $\mathscr{S}_{K_0}$ there exists a finite extension K of K_0 and finite extensions E_1, E_2, and L of K so that all the assumptions in Notation and Assumptions 4.1, 5.1, 6.1, 7.1, and 9.1 hold with respect to $\mathscr{S}_K$ and $\mathscr{A}_K$ – the sets of K-primes above $\mathscr{S}_{K_0}$ and $\mathscr{A}_{K_0}$ respectively. Further if $K_0 \neq \mathbb{Q}$ we can arrange that all the primes of $\mathscr{N}_{K_0} = \mathscr{A}_{K_0} \setminus \mathscr{S}_{K_0}$ lie above rational primes splitting completely in the extension $K_0/\mathbb{Q}$ so that if we remove one prime from $\mathscr{N}_{K_0}$ per every complete set of $\mathbb{Q}$-conjugates, the remaining set $\mathscr{L}_{K_0}$ will still be infinite.*

Proof. If we set K to be any number field containing $\mathbb{Q}(\cos(2\pi/q_1^{a_1} \dots q_k^{a_k}))$, where $a_i = 1$ if q_i is odd and $a_i = 2$ if $q_i = 2$, then any number field M with $K \subset M \subset K_\infty$ will have a subfield $\bar{M}$ such that $[M : \bar{M}] = q_i$ for some $i = 1, \dots, k$ and $M = \bar{M}(\cos(2\pi/q_i^{b_i}))$, where b_i is a positive integer and $2\cos(2\pi/q_i^{b_i}) = \xi_{i,b_i} + \xi_{i,b_i}^{-1}$ is an algebraic integer. Thus the assumptions that only finitely many primes divide the degrees of subextensions and the integral basis elements and their conjugates are bounded in absolute value hold. Further the condition on finite number of rational primes ramified in K_∞ also holds by our choice of K_∞.

Our next job is to make sure that primes of $\mathscr{S}_K$ do not split in the extensions K_∞/K. Since every prime can have only finitely many factors in K_∞ we can certainly choose a number field K contained in K_∞ so that it contained $\mathbb{Q}(\cos(2\pi/q_1^{a_1} \dots q_k^{a_k}))$, where $a_i = 1$ if q_i is odd and $a_i = 2$ if $q_i = 2$ and the maximum possible number of factors for each prime in $\mathscr{S}_{K_0}$. Then the primes of $\mathscr{S}_K$ will remain prime in the extension K_∞/K.

We now produce cyclic extensions E_1 and E_2 with the required properties. Choose two distinct odd rational prime numbers p_1 and p_2 such that each p_i is prime to $\prod(q_i - 1)q_i$. By Lemma 12.9, there exists a cyclic degree p_1 extension $\hat{E}_1$ of $\mathbb{Q}$ such that all the prime below $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ split completely in the extension $\hat{E}_1/\mathbb{Q}$. Also by Lemma 12.9, there exists a cyclic degree p_2 extension $\hat{E}_2$ of $\mathbb{Q}$ such that all the prime below $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ do not split in the extension $\hat{E}_2/\mathbb{Q}$. Now set $E_1 = K\hat{E}_1, E_2 = K\hat{E}_2$. Then, given the degrees of the extensions involved, by Lemmas 12.5 and 12.6 we have that $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ split completely in the extension E_1/K and do not split in the extension E_2/K. We also not here that since $\hat{E}_1$ and $\hat{E}_2$ are Galois extensions of $\mathbb{Q}$ of odd degree, they must be totally real.

We still have to construct L so that $\mathfrak{p}_i$'s split in L/K, choose a generator for H with the correct sign for the conjugates and make sure that the requirements for roots of unity are satisfied: LE_1K_∞ should have no roots of unity beyond ± 1 and $G_\infty E_2 H$ should not have any roots of unity which are not already in G_∞.

To make sure that LE_1K_∞ has no non-real roots of unity, it is enough, by Lemma 2.4 of [24] to make sure that in the extension LE_1/E_1 we have ramification of at least two K-primes lying above two different rational primes. We can do this by choosing $c \in K$ such that besides satisfying the inequality $\sigma(c) < 0$ for all embeddings σ of K into its algebraic closure and equivalencies $c \equiv 1 \mod \mathfrak{p}_i$, it is the case that c also satisfies the condition that it has order 1 at two K-primes lying above two different rational primes. Such an c can be found by the Weak Approximation Theorem. Now we can set $L = K(\sqrt{c})$.

Now note that by Lemma 12.9 we can make sure that no factor of $2, 3, q_1, \dots, q_k$ is ramified in the extension E_2/K. Let ℓ be the prime ramified in this extension and note that the ramification degree of ℓ is $p_2 < \ell - 1$. Next let's consider $G_\infty E_2$ and note that the only primes which are ramified in any finite subextension of this field are $q_1, \dots, q_k, \ell$.

Now choose $d \in O_K$ ($\sqrt{d}$ will generate H) so that $\sigma(d) > 0$ for all embeddings σ of K into its algebraic closure, $d \equiv 1 \mod 4$ and d is a unit at all the factors of $2, 3, q_1, \dots, q_k$ and ℓ. Now the only rational primes ramified in any finite subextension of $G_\infty H E_2$ are $q_1, \dots, q_k, \ell$, and factors of d. Thus, the only "extraneous" roots of unity which can occur are ξ_ℓ and ξ_t, where a factor of t divides d. But if $\xi_\ell \in G_\infty H E_2$, then for

some GHE_2 we must have ramification of ℓ in the extension equal to $\ell - 1$, which is not the case by the argument above. Similarly, if $\xi_t \in G_\infty HE_2$, then t must have ramification at least $t-1$ in some GHE_2. However, by construction, the ramification degree of t can be at most 2 and $t > 3$.

Now we are ready to choose $\mathscr{A}_{K_0}$. We will describe $\mathscr{N}_{K_0}$ and add $\mathscr{S}_{K_0}$ to the set. By Lemma 12.10 there exists an infinite set $\mathscr{N}_{\mathbb{Q}}$ of rational primes P such that

(1) P splits completely in the extension $K/\mathbb{Q}$ and therefore also in the extension $K_0/\mathbb{Q}$.
(2) No factor of P in K splits in the extension E_1E_2G/K.

Now let $\mathscr{N}_{K_0}$ consist of all the K_0-primes lying above the primes of $\mathscr{N}_{\mathbb{Q}}$.

Finally we note that since only finitely many primes divide the degrees of subextensions, i.e divisors of $\prod_{i=1}^{q} q_i(q-1)$, and all the subextensions are Galois. Therefore, by Corollary 3.8 we will be able to use Theorems 3.6 and 3.7 □

We are now ready for the following theorem.

Theorem 11.8. *Let G_∞ be an infinite cyclotomic extension of $\mathbb{Q}$ with finitely many ramified rational primes and finite ramification degree for 2. Let $K_0 \neq \mathbb{Q}$ be a totally real number field contained in G_∞. Then for some large subring $O_{K_0,\mathscr{R}_{K_0}}$ of K_0 its integral closure $O_{G_\infty,\mathscr{R}_{G_\infty}}$ in G_∞ satisfies the following conditions:*

(1) *$O_{G_\infty,\mathscr{R}_{G_\infty}} \cap \mathbb{Q} = O_{\mathbb{Q},\mathscr{S}_{\mathbb{Q}}}$, where $\mathscr{S}_{\mathbb{Q}}$ is finite.*
(2) *There exists a positive integer n and a polynomial $F(t,\bar{x}) \in K_0[t,\bar{x}]$ satisfying the following conditions. For any $t \in O_{G_\infty,\mathscr{R}_{G_\infty}}$, if there exists $\bar{x} \in (O_{K_\infty,\mathscr{R}_{G_\infty}})^n$ such that $F(t,\bar{x}) = 0$, then $t \in O_{G_\infty,\mathscr{R}_{G_\infty}} \cap \mathbb{Q}$. Further, if $t \in O_{G_\infty,\mathscr{R}_{G_\infty}} \cap \mathbb{Q}$, there exist $\bar{x} \in (O_{K_0,\mathscr{R}_{K_0}})^n$ such that $F(t,\bar{x}) = 0$. Thus $\mathbb{Z}$ is definable over $O_{G_\infty,\mathscr{R}_{G_\infty}}$.*

It is also possible to find a totally real number field $K \subset K_\infty$ such that the Dirichlet (or natural) density of $\mathscr{R}_K$ can be made arbitrarily close to 1/2.

Proof. This theorem follows almost immediately from Theorem 10.8 and Proposition 11.7, if we let K, $\mathscr{A}_{K_0}, \mathscr{L}_{K_0}$ be constructed as in Proposition 11.7 and set $\mathscr{R}_{K_0} = \mathscr{L}_{K_0} \cup \mathscr{S}_{K_0}$, since bounded ramification for 2 implies that Assumption 10.2 holds for some finite extension K of K_0. There is only one point which requires explanation: the question of density. We now show how the density of $\mathscr{A}_K$ can be arranged to be arbitrarily close to 1/2. Here we can assume that $K = K_0$ satisfies Assumption 10.2 and review the definition of $\mathscr{R}_K$. It can be formed in several steps. We start with $\mathscr{N}_K$– a set of K primes not splitting in the extensions E_1/K, E_2/K and G/K. Next out of $\mathscr{N}_K$ we form a set of K-primes $\mathscr{L}_K$ by removing the highest degree prime out of every complete set of $\mathbb{Q}$-conjugates in $\mathscr{L}_K$. Finally, we let $\mathscr{R}_K = \mathscr{L}_K \cup \mathscr{S}_K$. Here we note that if a number field K satisfies the assumptions of Theorem 10.8, then so does any finite extension of K inside K_∞. Hence when required we can make the degree of K arbitrarily large. We start with the fact that, by Tchebotarev Density Theorem (the classic or natural versions), the density (Dirichlet or natural) of primes of K not splitting in the extension G/K is 1/2. However, out of this set of K-primes we have to remove the primes splitting either in E_1 (density $1/p_1$) or E_2 (density $1/p_2$) and primes of the highest relative degree in complete sets of $\mathbb{Q}$-conjugates. Since the only primes which contribute to density are primes of relative degree 1 over $\mathbb{Q}$, we should worry only about complete conjugates sets lying above rational primes splitting completely in the extension $K/\mathbb{Q}$. The density of the set containing exactly one prime for each complete set of conjugates lying above a completely splitting rational prime is $\frac{1}{[K:\mathbb{Q}]}$. Using Tchebotarev Density Theorem and a Galois extension $GE_1E_2/\mathbb{Q}$ one can deduce that the set of removed primes has density (natural and Dirichlet), and by making the degree of K over $\mathbb{Q}$, and the degrees of E_1, and E_2 over K high enough we can make this density arbitrarily small.

□

We now extend results above to complex number fields contained in G_∞.

Corollary 11.9. *Let G_0 be a number field contained in G_∞. Then for some large subring $O_{G_0,\mathscr{R}_{G_0}}$ of G_0, its integral closure $O_{G_\infty,\mathscr{R}_{G_\infty}}$ in G_∞ satisfies the following conditions:*

(1) *$O_{G_\infty,\mathscr{R}_{G_\infty}} \cap \mathbb{Q} = O_{\mathbb{Q},\mathscr{S}_{\mathbb{Q}}}$, where $\mathscr{S}_{\mathbb{Q}}$ is finite.*
(2) *There exists a positive integer n and a polynomial $F(t,\bar{x}) \in G_0[t,\bar{x}]$ satisfying the following conditions. For any $t \in O_{G_\infty,\mathscr{R}_{G_\infty}}$, if there exists $\bar{x} \in (O_{K_\infty,\mathscr{R}_{G_\infty}})^n$ such that $F(t,\bar{x}) = 0$, then*

$t \in O_{G_\infty,\mathscr{R}_{G_\infty}} \cap \mathbb{Q}$. Further, if $t \in O_{G_\infty,\mathscr{R}_{G_\infty}} \cap \mathbb{Q}$, there exist $\bar{x} \in (O_{G_0,\mathscr{R}_{G_0}})^n$ such that $F(t,\bar{x}) = 0$. Thus $\mathbb{Z}$ is definable over $O_{G_\infty,\mathscr{R}_{G_\infty}}$.

Proof. Either G_0 is totally real and we are done, or G_0 is an extension of degree 2 of some totally real number field K_0. In the latter case construct $O_{K_0,\mathscr{R}_{K_0}}$ as in Theorem 11.8 and let $O_{G_0,\mathscr{R}_{G_0}}$ be the integral closure $O_{K_0,\mathscr{R}_{K_0}}$ in G_0. □

Our next goal is to apply results above to small rings – rings of $\mathscr{S}$-integers with finitely many primes in $\mathscr{S}$. To obtain the most general results we need a technical lemma.

Lemma 11.10. *As above let G/K to be an extension of degree 2 generated by $\alpha \in O_G$, and let $\mathscr{C}_G$ be a set of G-primes such that no prime of $\mathscr{C}_G$ has its K-conjugate in $\mathscr{C}_G$ (thus $O_{G,\mathscr{C}_G} \cap K = O_K$). Let $\mathscr{S}_K$ be the set of all the K-primes of lying below the primes of $\mathscr{C}_G$. Let $O_{K_\infty,\mathscr{S}_{K_\infty}}, O_{G_\infty,\mathscr{C}_{G_\infty}}$ be the integral closures of $O_{K,\mathscr{S}_K}$ and $O_{G,\mathscr{C}_G}$ respectively. Next let $\mathbf{A} \subset O_{K_\infty}$ and be such that $O_K \subset \mathbf{A}$. Now consider the following set*

$$\mathbf{B} = \{\frac{x}{y} : x, y \in \mathbf{A} \wedge (\exists a, b, c, d, e, f \in O_{K_\infty})(cde \neq 0 \wedge (e, f) = 1 \wedge \frac{a}{c} + \alpha\frac{b}{d} \in O_{G_\infty,\mathscr{C}_{G_\infty}} \wedge 2\frac{a}{c} = \frac{e}{f} \wedge \frac{fx}{y} \in \mathbf{A}\}.$$

We claim that $O_{K,\mathscr{S}_K} \subset \mathbf{B} \subset O_{K_\infty,\mathscr{S}_{K_\infty}}$.

Proof. Let $\mathfrak{p}_K \in \mathscr{S}_K$, let $\mathfrak{p}_G \in \mathscr{C}_G$ be a prime above $\mathfrak{p}_K$ in G, and let $m \in \mathbb{Z}_{>0}$ be a multiple of the class numbers of K and G . Then there exists $a, c, b, d \in O_K, cd \neq 0$ such that

$$\frac{a}{c} + \alpha\frac{b}{d} \in O_{G,\mathscr{C}_G}$$

and

$$\mathrm{ord}_{\mathfrak{p}_G}\left(\frac{a}{c} + \alpha\frac{b}{d}\right) = -m,$$

while being integral at all the other primes. Since $\bar{\mathfrak{p}}_G$ - the conjugate of $\mathfrak{p}_G$ over K, is not in $\mathscr{C}_G$, we conclude that

$$\mathrm{ord}_{\bar{\mathfrak{p}}_G}\left(\frac{a}{c} + \alpha\frac{b}{d}\right) = \mathrm{ord}_{\mathfrak{p}_G}\left(\frac{a}{c} - \alpha\frac{b}{d}\right) = 0.$$

Consequently,

$$\mathrm{ord}_{\mathfrak{p}_K}\left(\frac{2a}{c}\right) = \mathrm{ord}_{\mathfrak{p}_G}\left(\frac{a}{c} + \alpha\frac{b}{d}\right) = -m.$$

Using the finiteness of the K-class number again, we can find $e, f \in O_K$ such that $(e, f) = 1$ and $\frac{e}{f} = \frac{2a}{b}$. Then we conclude that

$$\mathrm{ord}_{\mathfrak{p}_K} f = -\mathrm{ord}_{\mathfrak{p}_K}\left(\frac{2a}{c}\right) = -\mathrm{ord}_{\mathfrak{p}_G}\left(\frac{a}{c} + \alpha\frac{b}{c}\right) = m.$$

Hence, if $\frac{x}{y} \in O_{K,\mathscr{S}_K}$, then there exists f as above (essentially the K-"denominator" of an element of $O_{G,\mathscr{C}_G}$) so that $\frac{fx}{y} \in \mathbf{A}$.

Conversely, suppose $\frac{a}{c} + \alpha\frac{b}{d} \in GM \cap O_{G_\infty,\mathscr{C}_{G_\infty}}$ for some finite extension M of K in K_∞ and $\mathrm{ord}_{\mathfrak{p}_M} f < 0$ for some prime of M, where a, b, c, d, e, f are as described in the statement of the lemma. Then $\mathrm{ord}_{\mathfrak{p}_M}\frac{e}{f} = \mathrm{ord}_{\mathfrak{p}_M}(2\frac{a}{c}) < 0$, and consequently $\mathfrak{p}_M \in \mathscr{S}_M$. So if $\frac{fx}{y} \in \mathbf{A} \subset O_{K_\infty}$, then $\frac{x}{y} \in O_{K_\infty,\mathscr{S}_\infty}$. □

Remark 11.11. A more natural way to state the lemma above would be to assert that for some set $\mathbf{B}$ such that $O_{K,\mathscr{S}_K} \subset \mathbf{B} \subset O_{K,\mathscr{S}_{K_\infty}}$ we have that $\mathbf{B} \leq_{Dioph} \mathbf{A} \leq_{Dioph} O_{G_\infty,\mathscr{C}_{G_\infty}}$. (For a discussion of Diophantine generation see either [23] or [31].)

We are now ready to deal with rings of $\mathscr{S}$-integers where $\mathscr{S}$ is finite, also known as "small" rings.

Theorem 11.12. *Let G_∞ be a cyclotomic extension of $\mathbb{Q}$ with finitely many ramified rational primes. Let R be any number field contained in G_∞ and let $\mathscr{S}_R$ be a non-empty finite set of primes of R. Then there exists a positive integer n and a polynomial $F(t, \bar{x}) \in K[t, \bar{x}]$ satisfying the following conditions. For any $t \in O_{G_\infty, \mathscr{S}_{G_\infty}}$, if there exists $\bar{x} \in (O_{K_\infty, \mathscr{S}_{G_\infty}})^n$ such that $F(t, \bar{x}) = 0$, then $t \in O_{G_\infty, \mathscr{S}_{G_\infty}} \cap \mathbb{Q}$. Further, if $t \in O_{G_\infty, \mathscr{S}_{G_\infty}} \cap \mathbb{Q}$, there exist $\bar{x} \in (O_{R, \mathscr{S}_R})^n$ such that $F(t, \bar{x}) = 0$. Thus, $O_{G_\infty, \mathscr{S}_{G_\infty}} \cap \mathbb{Q}$ is definable over $O_{G_\infty, \mathscr{S}_{G_\infty}}$. Consequently $\mathbb{Z}$ is existentially definable in the integral closure of $O_{R, \mathscr{S}_R}$ in G_∞ and Hilbert's Tenth Problem is not decidable over $O_{G_\infty, \mathscr{S}_{G_\infty}}$.*

Proof. If the number field where we select the ring of $\mathscr{S}$-integers is totally real (a field K in our notation), then the assertion of the theorem follows directly from Theorem 11.8. If, however, the field is totally complex (a field G in our notation), we have to be more carefully. Let $\mathscr{C}_G$ and $O_{G_\infty, \mathscr{C}_{G_\infty}}$ be defined as above. Since the construction of a Diophantine definition of $O_{K_\infty, \mathscr{S}_{K_\infty}}$ over $O_{G_\infty, \mathscr{S}_{G_\infty}}$, where $\mathscr{S}_K$ is defined as usual to be a finite set of primes of some totally real number field K lying below primes of $\mathscr{C}_G$ with $[G : K] = 2$, was carried out over the ring of integers, while we "neutralized" the "denominators" by using a polynomial $Q(X)$ and the fact that all the primes allowed in the denominator of the divisors of elements of the rings in question did not split in the extension $E_2 G_\infty / K_\infty$ (see Section 5 and Lemma 7.3), we can replicate this process no matter what finite set of primes of G we select. However, the difficulty can arise when we find ourselves in K_∞. In order to carry out the totally real part of the construction we need at least one "prime in the denominator", i.e. if $O_{G_\infty, \mathscr{C}_{G_\infty}} \cap K_\infty = O_{K_\infty}$ we will not be able to proceed directly. We need somehow to construct $O_{K, \mathscr{S}_K}$ so that we have solutions to norm equations (4.1). To show that this can be in fact be done, we use Lemma 11.10. We note that a set $\mathbf{A}$, as described in the statement of the lemma is indeed Diophantine over $O_{G_\infty, \mathscr{C}_{G_\infty}}$ and Lemma 11.10 then tells us that using polynomial equations we can represent elements of a set $\mathbf{B}$ containing $O_{K, \mathscr{S}_K}$. Consequently, the totally real part of the construction can be carried out.

Finally we note that being non-zero and relatively prime in a ring of integers are Diophantine conditions by Propositions 2.3 and 2.4. □

We now can make use of Kronecker-Weber Theorem and Lemma 12.3 to assert the following.

Theorem 11.13. *Let A_∞ be an abelian extension of $\mathbb{Q}$ with finitely many ramified rational primes. Then the following statements are true.*

- *If the ramification degree of 2 is finite, then for any number field $X \subset A_\infty$ there exists an infinite set of X-primes $\mathscr{W}_X$ such that $\mathbb{Z}$ is existentially definable in the integral closure of $O_{X, \mathscr{W}_X}$ of A_∞.*
- *For any number field $X \subset A_\infty$ and any finite non-empty set $\mathscr{S}_X$ of its primes we have that $\mathbb{Z}$ is existentially definable in the integral closure of $O_{X, \mathscr{S}_X}$ in A_∞.*

Proof. Let A_∞ be an abelian equation with finitely many ramified primes, and assume that the ramification degree of 2 is finite (possibly 1). Then by Lemma 12.3 we have that $A_\infty \subset G_\infty = \mathbb{Q}(\xi_{1,r}, \{\xi_{i,j}, i = 2, \ldots, k, j \in \mathbb{Z}_{>0}\})$, where $p_1 = 2$ and r is a positive integer. Now the theorem follows from Corollary 11.9 and Theorem 11.12 via polynomials $F(t, \bar{x})$. □

Remark 11.14. While infinite abelian and infinite cyclotomic extensions with finitely many ramified rational primes are probably the "nicest" examples of the fields to which our results apply, they are certainly not the only ones. One can produce more examples by starting with a totally real subfield of an infinite cyclotomic with finitely many ramified rational primes, attaching it to an arbitrary totally real number field and then adding an arbitrary extension of degree 2.

12. Appendix

This section contains some technical results used in the paper. This first lemma is a modification of Lemma 8.1 of [30].

Lemma 12.1. *Let K be a real number field. Let $F(T) \in K[T]$ be a polynomial of degree $n > 0$. Suppose that for some positive numbers $l_0, l_1, \ldots, l_k, k < n$, we have that polynomials $F(T+l_0), F(T+l_1), \ldots, F(T+l_k)$ are linearly independent over $\mathbb{C}$. Then there exist a positive constant C such that for any real $l > C$, polynomials $F(T + l_0), F(T + l_1), \ldots, F(T + l_k), F(T + l)$ are also linearly independent over $\mathbb{C}$.*

Proof. Let $F(T) = a_0 + a_1T + \ldots a_nT^n$. Then for $l \in \mathbb{N}$ we have that

$$F(T+l) = a_0 + a_1(T+l) + \ldots + a_n(T+l)^n =$$

$$a_0 + a_1(T+l) + \ldots + a_i\left(\sum_{j=0}^{i}\left(\begin{array}{c} i \\ j \end{array}\right)T^j l^{i-j}\right) + \ldots + a_n\left(\sum_{j=0}^{n}\left(\begin{array}{c} n \\ j \end{array}\right)T^j l^{n-j}\right) =$$

$$\sum_{j=0}^{n} a_j l^j + \ldots + \left(\sum_{j=k}^{n}\left(\begin{array}{c} j \\ k \end{array}\right)a_j l^{j-k}\right)T^k + \ldots + a_nT^n =$$

$$P_n(l) + P_{n-1}(l)T + \ldots P_0(l)T^n, \tag{12.14}$$

where $P_i(l) \in K[l]$ is a polynomial of degree i in l. (The coefficient of l^i in $P_i(l)$ is $a_n \neq 0$ by assumption on the degree of $F(T)$.) Let $F_k(T+l) = \sum_{j=0}^{k} P_j(l)T^{n-j}$. Suppose now that we found $l_0, \ldots, l_k, k < n$ such that $F_k(T), F_k(T+l_1), \ldots, F_k(T+l_k)$ are linearly independent over $\mathbb{R}$. Let $l \in \mathbb{N}$ be such that $F_{k+1}(T+l) = \sum_{i=0}^{k} A_i F_{k+1}(T+l_i), A_i(l) = A_i \in \mathbb{C}$. Then, we have a linear system

$$P_j(l) = \sum_{i=0}^{k} A_i P_j(l_i), j = 0, \ldots, k+1. \tag{12.15}$$

We can solve the first $k+1$ equations simultaneously for A_i using Cramer's rule. Thus,

$$A_i = \frac{\sum_{j=0}^{k} b_j P_j(l)}{\det(P_j(l_i))},$$

where $\det(P_j(l_i)), j = 0, \ldots, k, i = 0, \ldots, k$ is not zero by induction hypothesis and $b_j \in \mathbb{C}$. Therefore, for each $i = 0, \ldots, k$, we have that $A_i = A_i(l)$ is a fixed polynomial in l of degree at most k. Next consider the equation of system (12.15) number $k+2$.

$$P_{k+1}(l) = \sum_{i=0}^{k} A_i(l) P_{k+1}(l_i).$$

Note that on the left we have a polynomial in l of degree $k+1$ and on the right a polynomial of degree at most k. Thus, the equality will not hold for all sufficiently large l. Finally, note that for any non-negative integer $k \leq n$, any $l_0, \ldots, l_k \in \mathbb{R}$, we have that the set $\{F(T+l_0), \ldots, F(T+l_k)\}$ is linearly dependent only if the set $\{F_k(T+l_0), \ldots, F_k(T+l_k)\}$ is linearly dependent. □

The next lemma deals with degrees of certain extensions used to define integrality at finite sets of primes.

Lemma 12.2. *Let K be a field. Let q be a rational prime. Let $b \in K$ be such that b is not a q-th power in K. Let β, an element of the algebraic closure of K, be a root of $X^q - b$. Then $[K(\beta) : K] = q$.*

Proof. It is obvious that $[K(\beta) : K] \leq q$. So suppose $[K(\beta) : K] = m < q$. Let $\beta_1 = \beta, \ldots, \beta_m$ be all the conjugates of β over K. Observe that $\beta_i = \xi_i\beta$, where ξ_i is a q-th root of unity. Further let

$$c = \mathbf{N}_{K(\beta)/K} = \prod_{i=1}^{m} \xi_i\beta_i = \xi\beta^m \in K,$$

where ξ is again a q-th root of unity. Now let $x, y \in \mathbb{Z}$ be such that $xm + yq = 1$. Then

$$c^x b^y = \xi^x \beta^{xm} \beta^{qy} = \xi'\beta \in K,$$

where ξ' is another q-th root of unity. But $(\xi'\beta)^q = b$ in contradiction of our assumption on b. □

The next lemma uses the Kronecker-Weber Theorem to determine how to embed an abelian extension into the smallest possible cyclotomic one.

Lemma 12.3. *Let A_∞ be an abelian extension of $\mathbb{Q}$ with finitely many ramified rational primes $p_1, \ldots, p_k$. Then A_∞ is contained in the $F = \mathbb{Q}(\xi_{1,l}, \ldots, \xi_{k,l}, l \in \mathbb{Z}_{>0})$, where for $i = 1, \ldots, k, j \in \mathbb{Z}_{>0}$ we have that $\xi_{i,j}$ is p_i^j-th primitive root of unity.*

Proof. Suppose the assertion of the lemma does not hold. By Kronecker-Weber theorem, A_∞ must be contained in a cyclotomic extension. Then for some $\alpha \in A_\infty$ we have that $\alpha \notin F$ but $\alpha \in F(\xi_n)$, where ξ_n is an n-th primitive root of unity and $(n, p_i) = 1$ for $i = 1, \ldots, k$. Observe that the only rational primes ramified in the extension $F(\alpha)/\mathbb{Q}$ are $p_1, \ldots, p_k$ (see Proposition 8, Section 4, Chapter II of [9]). Next consider $F(\xi_n)/F$ and let $\tau \in \mathrm{Gal}(F(\xi_n)/F)$ be such that $F(\alpha)$ is the fixed field of the subgroup generated by τ. Since F and $\mathbb{Q}(\xi_n)$ are linearly disjoint over $\mathbb{Q}$, we have that $\mathrm{Gal}(F(\xi_n)/F) \overrightarrow{\cong} \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ with the isomorphism realized by restriction. Therefore, restriction of τ to $\mathbb{Q}(\xi_n)$ will not generate all of $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$. Let $\mu \in \mathbb{Q}(\xi_n)$ generate the fixed field of the subgroup of $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ generated by restriction of τ to $\mathbb{Q}(\xi_n)$. Then $\mu \notin \mathbb{Q}$ and $\mu \in F(\alpha)$. Hence $\mathbb{Q}(\mu) \subset F(\alpha)$. But one of the rational divisors of n is ramified in the extension $\mathbb{Q}(\mu)/\mathbb{Q}$ contradicting our assumption on A_∞. □

The following lemmas will all deal with some technical aspects of prime splitting in number fields.

Lemma 12.4. *Let T/K be a cyclic extension of number fields, and let M be an extension of K such that it is Galois and $([M : K], [T : K]) = 1$. Let $\mathfrak{p}_K$ be a prime of K not splitting in the extension T/K. Let $\mathfrak{p}_M$ be an M-prime above $\mathfrak{p}_K$. Then $\mathfrak{p}_M$ does not split in the extension MT/M.*

Proof. First of all observe that the extension MT/K is Galois and every factor of $\mathfrak{p}_K$ in M has the same number of factors in MT. If this number is not 1 then it is a non trivial divisor of $[MT : M] = [T : K]$. Thus, if the factors of $\mathfrak{p}_K$ do not stay prime in the extension MT/M, the number of MT-factors of $\mathfrak{p}_K$ has a non-trivial common divisor with $[T : K]$. On the other hand, since $\mathfrak{p}_K$ does not split in the extension T/K, the number of MT-factors of $\mathfrak{p}_K$ is a divisor of $[MT : T] = [M : K]$. Thus, if some factor of $\mathfrak{p}_K$ splits in the extension MT/M, we have a contradiction of our assumption on the degrees of extensions M/K and T/K. □

Lemma 12.5. *Let K/B be a Galois extension and let T/B be a cyclic extension. Assume further that K and T are linearly disjoint over B. Let $\mathfrak{p}_B$ be a B-prime not splitting in the extension T/B and splitting completely in the extension K/B. Then the following statements are true.*

1. *There are infinitely many primes of B satisfying the two requirements for $\mathfrak{p}_B$.*
2. *Let $\mathfrak{p}_K$ be a K-prime lying above a B-prime $\mathfrak{p}_B$ as above. Then $\mathfrak{p}_K$ does not split in the extension TK/K.*

Proof. The linear disjointness implies that

$$\mathrm{Gal}(KT/B) \cong \mathrm{Gal}(KT/T) \times \mathrm{Gal}(KT/K) \overrightarrow{\cong} \mathrm{Gal}(K/B) \times \mathrm{Gal}(T/B),$$

where the last isomorphism is realized by restriction. So consider an element $(\mathrm{id}_K, \sigma_T) \in \mathrm{Gal}(KT/B)$, where id_K is the identity element of $\mathrm{Gal}(K/B)$ and σ_T is a generator of $\mathrm{Gal}(T/B)$. Let $\mathfrak{p}_{KT}$ be a KT-prime whose Frobenius isomorphism is $(\mathrm{id}_K, \sigma_T)$. By Tchebotarev density theorem there are infinitely many such primes. Next let $\mathfrak{p}_K$ be a prime K prime below it. The decomposition group of $\mathfrak{p}_{KT}$ over K is the intersection of the decomposition group of $\mathfrak{p}_{KT}$ over B and $\mathrm{Gal}(KT/K)$. This intersection is all of $\mathrm{Gal}(KT/K)$ and therefore $\mathfrak{p}_K$ will not split in the extension KT/K. Finally, since the decomposition groups of $\mathfrak{p}_{KT}$ over K and over B are the same, we conclude that the decomposition group of $\mathfrak{p}_K$ over B is trivial. Thus, if $\mathfrak{p}_B$ is the B-prime below $\mathfrak{p}_{KT}$, then $\mathfrak{p}_B$ splits completely in the extension K/B.

Next let $\mathfrak{p}_B$ be as above and let $\mathfrak{p}_{KT}$ be its factor in KT. Then, since the relative degree of $\mathfrak{p}_T$ over $\mathfrak{p}_B$, $f(\mathfrak{p}_T/\mathfrak{p}_B) = [T : B]$, we have that $[T : B] \geq f(\mathfrak{p}_{KT}/\mathfrak{p}_B) = f(\mathfrak{p}_{KT}/\mathfrak{p}_K) f(\mathfrak{p}_K/\mathfrak{p}_B) = f(\mathfrak{p}_{KT}/\mathfrak{p}_K) \leq [T : B]$, where the last equality holds because $\mathfrak{p}_B$ splits completely in K. Thus, $f(\mathfrak{p}_{KT}/\mathfrak{p}_K) = [T : B]$ and $\mathfrak{p}_K$ remains prime in KT. □

Lemma 12.6. *Let K/B be a finite extension of number fields and let T/B be a Galois extension. Assume further that K and T are linearly disjoint over B. Let $\mathfrak{q}_B$ be a B-prime splitting completely (into distinct factors) in the extension T/B. Let $\mathfrak{q}_K$ be a K-prime lying above $\mathfrak{q}_B$. Then $\mathfrak{q}_K$ splits in the extension TK/K.*

Proof. In this case the linear disjointness implies that

$$\mathrm{Gal}(KT/K) \overrightarrow{\cong} \mathrm{Gal}(T/B),$$

where the isomorphism, as above, is realized by restriction. Let $\sigma \in \mathrm{Gal}(KT/K)$ be the Frobenius isomorphism of some KT-factor of $\mathfrak{q}_K$. Then σ restricted to elements of T should be an element of the decomposition group of $\mathfrak{q}_T$, a factor of $\mathfrak{q}_B$ in T. But the decomposition group of any factor of $\mathfrak{q}_B$ in T is trivial. Thus, since the restriction to B is an isomorphism, we conclude that the decomposition group of any factor of $\mathfrak{q}_K$ in KT is trivial. Thus $\mathfrak{q}_K$ splits completely. □

Lemma 12.7. *Let U/K be a Galois extension of number fields. Let $F_i/U, i = 1, \ldots, k$ be a cyclic number field extension such that each F_j is linearly disjoint from $\prod_{i \neq j} F_i$ and the extension $\left(\prod_{i=1}^k F_i\right)/K$ is Galois. Then there are infinitely many primes of U not splitting in the extension F_i/U for any i and lying above a prime of K splitting completely in U.*

Proof. The linear disjointness condition implies that $\mathrm{Gal}(\prod_{i=1}^k F_i/U) \cong \prod_{i=1}^k \mathrm{Gal}(F_i/U)$. Let σ_i be a generator of $\mathrm{Gal}(F_i/U)$. Then any prime of $\prod_{i=1}^k F_i$ whose Frobenius is $(\sigma_1, \ldots, \sigma_n) \in \mathrm{Gal}(\prod_{i=1}^k F_i/U) \subset \mathrm{Gal}(\prod_{i=1}^k F_i/K)$ will have the desired property. Now Tchebotarev Density Theorem tells us that there are infinitely many such primes. □

The following two lemmas are slight generalizations of Lemma 2.6 of [18].

Lemma 12.8. *Let F/U be a cyclic extension such that for some rational prime q we have that $[F : U] = \ell \equiv 0 \mod q$. Let N be the unique q-th degree extension of U contained in F. Let $\mathfrak{p}_F$ be a prime of F and let $\mathfrak{p}_U$ be the U-prime below it. Let σ be the Frobenius automorphism of $\mathfrak{p}_F$. Then $\mathfrak{p}_U$ splits in N if and only if σ is a q-th power in $Gal(F/U)$.*

Proof. The unique index q subgroup H of $\mathrm{Gal}(F/U)$ consists of q-th powers. Further, N is the fixed field of H. Suppose now that $\sigma \in H$. Then the decomposition group of $\mathfrak{p}_F$ over U (denoted by $G_{\mathfrak{p}_F}(F/U)$) and N (denoted by $G_{\mathfrak{p}_F}(F/N)$) are the same. Let $\mathfrak{p}_N$ be the N-prime below $\mathfrak{p}_F$. In this case the decomposition group of $\mathfrak{p}_N$ over U, equal to $G_{\mathfrak{p}_F}(F/U)/G_{\mathfrak{p}_F}(F/N)$, is trivial and $\mathfrak{p}_U$ splits completely in N. Conversely, suppose $\sigma \notin H$. Then $G_{\mathfrak{p}_F}(F/N) \neq G_{\mathfrak{p}_F}(F/U)$ and $G_{\mathfrak{p}_F}(F/U)/G_{\mathfrak{p}_F}(F/N)$ is not trivial. Thus, $\mathfrak{p}_U$ does not split completely in the extension N/U. Since the degree of the extension is prime, however, for an unramified prime not splitting completely is equivalent to staying prime. □

Lemma 12.9. *Let $p_1, \ldots, p_k, t$ be a finite set of distinct rational primes. Then there exists a totally real cyclic extension of $\mathbb{Q}$ of degree t where none of p_i's splits and there exists a totally real cyclic extension of $\mathbb{Q}$ of degree t where all of p_i split. Further, we can arrange for any given finite subset of primes not to ramify in these extensions.*

Proof. Let ℓ be a prime splitting completely into distinct factors in the extension $\mathbb{Q}(\xi_t, \sqrt[t]{p_1}, \ldots, \sqrt[t]{p_k})$, where ξ_t is a primitive t-th root of unity. Then $\ell \equiv 1 \mod t$ and $\mod \ell$ we have that p_i is a t-th power. Now consider the extension $\mathbb{Q}(\xi_\ell)/\mathbb{Q}$, where ξ_ℓ a primitive ℓ-th root of unity. Let τ_i be the Frobenius of p_i. Then $\tau_i(\xi_\ell) = \xi_\ell^{p_i}$ and τ_i is a t-th power in $\mathrm{Gal}(\mathbb{Q}(\xi_\ell)/\mathbb{Q})$. Let G be the unique degree t extension of $\mathbb{Q}$ inside of $\mathbb{Q}(\xi_\ell)$. Then by Lemma 12.8 we have that p_i splits completely in this extension, and the first assertion of the lemma holds.

Now let ℓ satisfy the following conditions:

(1) ℓ splits completely in $\mathbb{Q}(\xi_t)/\mathbb{Q}$.
(2) Factors of ℓ in $\mathbb{Q}(\xi_t)$ do not split in any of the extensions $\mathbb{Q}(\xi_t, \sqrt[t]{p_i})/\mathbb{Q}(\xi_t)$. (By Lemma 12.7 there are infinitely many such ℓ's.)

Then we conclude that as above $\ell \equiv 1 \mod t$, but p_i is not a t-th power mod ℓ. Now considering the extension $\mathbb{Q}(\xi_\ell)/\mathbb{Q}$ as above, by Lemma 12.8, we conclude that none of p_i will split in the unique degree t extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\xi_\ell)$.

Finally we observe that ℓ would be the only prime ramifying in either extension, and in choosing ℓ we can always avoid any finite set of primes. □

Lemma 12.10. *Let Z be a number field and let K/Z be a finite extension. Let $\beta \in \tilde{\mathbb{Q}}$ be such that $\beta^2 \in K$, $\beta \notin K$ and $K(\beta)/Z$ is Galois. Let E be a cyclic extension of Z of odd degree l with $(l, [K : Z]) = 1$. Then there exists an infinite set $\mathscr{B}_Z$ of primes of Z such that every K-prime above a prime of $\mathscr{B}_Z$ does not split in the extension $KE(\beta)/K$ and every prime in $\mathscr{B}_Z$ splits completely in the extension K/Z.*

Proof. Given our assumptions on the degrees of the extensions, $\mathrm{Gal}(KE(\beta)/K) = \mathrm{Gal}(K(\beta)/K)\times\mathrm{Gal}(E/Z)$. Let σ be the generator of $\mathrm{Gal}(K(\beta)/K)$ and let τ be a generator of $\mathrm{Gal}(E/Z)$. Let $\mathfrak{p}_{EK(\beta)}$ be a prime of $EK(\beta)$ whose Frobenius is $(\sigma,\tau) \in \mathrm{Gal}(EK(\beta)/Z)$. Note that (σ,τ) generates $\mathrm{Gal}(EK(\beta)/K)$ and therefore, if we let $\mathfrak{p}_K$ be the prime below $\mathfrak{p}_{EK(\beta)}$ in K we will have that $\mathfrak{p}_K$ does not split in the extension $KE(\beta)/K$. Next let $\mathfrak{q}_K$ be the conjugate of $\mathfrak{p}_K$ over Z. Since $KE(\beta)/Z$ is Galois, $\mathfrak{q}_K$ remains prime in the extension $KE(\beta)/K$ also. Let $\mathfrak{p}_Z$ be the Z-prime below $\mathfrak{p}_K$ and $\mathfrak{q}_K$. Then no factor of $\mathfrak{p}_Z$ in K splits in the extension $KE(\beta)/K$. Finally we note that the decomposition group of $\mathfrak{p}_{EK(\beta)}$ over K and over Z are the same. Thus, $\mathfrak{p}_Z$ must split completely in the extension K/Z. □

References

[1] Jean-Louis Colliot-Thélène, Alexei Skorobogatov, and Peter Swinnerton-Dyer. Double fibres and double covers: Paucity of rational points. *Acta Arithmetica*, 79:113–135, 1997.

[2] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi. Division-ample sets and diophantine problem for rings of integers. *Journal de Théorie des Nombres Bordeaux*, 17:727–735, 2005.

[3] Gunther Cornelissen and Karim Zahidi. Topology of diophantine sets: Remarks on Mazur's conjectures. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pages 253–260. American Mathematical Society, 2000.

[4] Martin Davis. Hilbert's tenth problem is unsolvable. *American Mathematical Monthly*, 80:233–269, 1973.

[5] Martin Davis, Yuri Matiyasevich, and Julia Robinson. Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution. In *Proc. Sympos. Pure Math.*, volume 28, pages 323– 378. Amer. Math. Soc., 1976.

[6] Jan Denef. Hilbert's tenth problem for quadratic rings. *Proc. Amer. Math. Soc.*, 48:214–220, 1975.

[7] Jan Denef. Diophantine sets of algebraic integers, II. *Transactions of American Mathematical Society*, 257(1):227– 236, 1980.

[8] Jan Denef and Leonard Lipshitz. Diophantine sets over some rings of algebraic integers. *Journal of London Mathematical Society*, 18(2):385–391, 1978.

[9] Serge Lang. *Algebraic Number Theory*. Addison Wesley, Reading, MA, 1970.

[10] Barry Mazur. The topology of rational points. *Experimental Mathematics*, 1(1):35–45, 1992.

[11] Barry Mazur. Questions of decidability and undecidability in number theory. *Journal of Symbolic Logic*, 59(2):353–371, June 1994.

[12] Barry Mazur. Speculation about the topology of rational points: An up-date. *Asterisque*, 228:165–181, 1995.

[13] Barry Mazur. Open problems regarding rational points on curves and varieties. In A. J. Scholl and R. L. Taylor, editors, *Galois Representations in Arithmetic Algebraic Geometry*. Cambridge University Press, 1998.

[14] Thanases Pheidas. Hilbert's tenth problem for a class of rings of algebraic integers. *Proceedings of American Mathematical Society*, 104(2):611–620, 1988.

[15] Bjorn Poonen. Elliptic curves whose rank does not grow and Hilbert's Tenth Problem over the rings of integers. Private Communication.

[16] Bjorn Poonen. Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers. In C. Fieker and D. Kohel, editors, *Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Computer Science*, pages 33–42. Springer Verlag, 2002.

[17] Bjorn Poonen. Hilbert's Tenth Problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *Journal of AMS*, 16(4):981–990, 2003.

[18] Bjorn Poonen and Alexandra Shlapentokh. Diophantine definability of infinite discrete non-archimedean sets and diophantine models for large subrings of number fields. *Journal für die Reine und Angewandte Mathematik*, 2005:27–48, 2005.

[19] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[20] Harold Shapiro and Alexandra Shlapentokh. Diophantine relations between algebraic number fields. *Communications on Pure and Applied Mathematics*, XLII:1113–1122, 1989.

[21] Alexandra Shlapentokh. Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem. To appear in Transactions of AMS.

[22] Alexandra Shlapentokh. Extension of Hilbert's tenth problem to some algebraic number fields. *Communications on Pure and Applied Mathematics*, XLII:939–962, 1989.

[23] Alexandra Shlapentokh. Diophantine classes of holomorphy rings of global fields. *Journal of Algebra*, 169(1):139–175, October 1994.

[24] Alexandra Shlapentokh. Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of $\mathbb{Q}$. *Annals of Pure and Applied Logic*, 68:299–325, 1994.

[25] Alexandra Shlapentokh. Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator. *Inventiones Mathematicae*, 129:489–507, 1997.

[26] Alexandra Shlapentokh. Hilbert's tenth problem over number fields, a survey. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pages 107–137. American Mathematical Society, 2000.

[27] Alexandra Shlapentokh. On diophantine decidability and definability in some rings of algebraic functions of characteristic 0. *Journal of Symbolic Logic*, 67(2):759–786, 2002.
[28] Alexandra Shlapentokh. On diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree 2. *Journal of Number Theory*, 95:227–252, 2002.
[29] Alexandra Shlapentokh. A ring version of Mazur's conjecture on topology of rational points. *International Mathematics Research Notices*, 2003:7:411–423, 2003.
[30] Alexandra Shlapentokh. On diophantine definability and decidability in some infinite totally real extensions of $\mathbb{Q}$. *Transactions of AMS*, 356(8):3189–3207, 2004.
[31] Alexandra Shlapentokh. *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. Cambridge University Press, 2006.

Department of Mathematics, East Carolina University, Greenville, NC 27858
E-mail address: shlapentokha@ecu.edu
URL: www.personal.ecu.edu/shlapentokha